Department of Defense
Public Key Infrastructure

DoD Approved External PKIs
Master Document

Version 5.9

May 18, 2016

Prepared for:

DoD PKI Program Management Office
9800 Savage Road
Suite 6718
Fort George G. Meade, MD 20755-6718

Prepared by:

Booz Allen Hamilton
8283 Greensboro Drive
McLean, Virginia 22102

Revision Page

Date	Version	Change Description
6/7/2011	1.0	Release 1.0
8/18/2011	1.1	Updated Treasury and ORC SSP sections, updated Department of State assurance level section, incorporated text comments, added additional VeriSign ECA CA, and added VeriSign NFI and ActivIdentity, Inc. NFI as a DoD approved PKIs.
10/05/2011	1.2	Added Citi NFI PKI and new DOD CAs 27-30 and DOD EMAIL CAs 27-30.
11/04/2011	1.3	Added Entrust NFI PKI as a DoD Approved External PKI
01/05/2012	2.0	Added Verizon Business NFI PKI as a DoD Approved External PKI Removed expired DoD [EMAIL] CAs 11,12,14
04/27/2012	2.1	Added ORC NFI PKI as a DoD Approved External PKI Removed expired DoD [EMAIL] CA 13 Removed expired Treasury Root CA and 3 Issuing CAs (OCIO, Fiscal, Treasury Public)
06/22/2012	2.2	Added new SHA-256 Dept. of State CA and updated Assurance Level information Added Boeing PKI as a DoD Approved External PKI Removed expired DoD [EMAIL] CA 15-18 and expired Entrust SSP SHA-1 chains
08/01/2012	2.3	Removed ActivIdentity NFI PKI as a DoD Approved External PKI Updated VeriSign NFI SHA-256 chain with US Senate and Millennium PIV-I CAs
02/13/2013	2.4	Added content for DoD [EMAIL] CA 31-32 and NPE CA 1-2 Updated VeriSign NFI PKI SHA-256 chain with Booz Allen and CSC SHA-256 PIV-I CAs Replaced expired Exostar FIS Certificate Authority
03/25/2013	2.5	Added Netherlands Ministry of Defence PKI as a DoD Approved External PKI
05/28/2013	3.0	Added Australian Defence Organisation (ADO) PKI as a DoD Approved External PKI Added content for DoD CCEB Interoperability Root CA 1
07/01/2013	3.1	Removed Citi NFI PKI as a DoD Approved External PKI Added content for Exostar FIS Signing CA 2 Issuing CA
09/05/2013	3.2	Renamed VeriSign NFI and SSP to Symantec NFI and SSP Updated Symantec NFI PKI SHA-256 chain with Eid Passport – RAPIDGate PIV-I CA
11/06/2013	3.3	Added content for HHS Intermediate CA under Entrust SSP Added content for Veterans Affairs Issuing CA under Treasury SSP Removed expired Treasury OCIO Issuing CA
01/01/2014	4.0	Removed expired SHA-1 content from ORC SSP and Symantec NFI/SSP PKIs.
02/20/2014	4.1	Added content for IdenTrust ECA 4
03/24/2014	4.2	Added content for Symantec Client ECA – G4 Added new Federal PKI Policy OID: id-fpki-common-piv-contentSigning
05/06/2014	4.3	Removed expired CAs: DoD [EMAIL] CA 19-20 and IdenTrust ECA 2. Updated CCEB IRCA 1 > ADOCA03 cross certificate Added content for additional Raytheon SHA-1 trust chain
06/10/2014	4.4	Added content for ORC ECA HW 5, ORC ECA SW 5, and ADOCA016 Removed expired content for ORC ECA HW 3 and ORC ECA SW 3

Revision Page (continued)

Date	Version	Change Description
07/01/2014	4.5	Added Exostar SHA-256 PKI as a DoD Approved External PKI, Removed expired content for VeriSign Client ECA – G2 Removed FPKI SHA-1 Authentication and CardAuth OIDs Removed SHA-1 OIDs from Symantec NFI and SSP, and Verizon Business SSP
08/01/2014	4.6	Added Cassidian NFI PKI as a DoD Approved External PKI Removed Exostar SHA-1 PKI as a DoD Approved External PKI Replaced ORC Root 2 with the Federal Common Policy CA (FCPCA) as trust anchor for ORC SSP Removed ORC SSP Inherited Policies from ORC Root 2
08/22/2014	4.6.1	Added Eid Passport – RAPIDGate Premier Issung CA (Symantec NFI)
02/02/2015	4.7	Removed expired CAs: DoD [EMAIL] CA 21-24 and ADOCA014
06/01/2015	5.0	Added content for DoD Root CA 3 and ECA Root CA 4 Added Northrop Grumman SHA-256 PKI as DoD Approved External PKI Added content for NRC Issuing CA (Symantec SSP) Added new FPKI OIDs: id-fpki-common-pivAuth-derived and id-fpki-common-pivAuth-derived-hardware Removed expired Raytheon trust chain
07/01/2015	5.1	Added content for re-keyed Treasury issuing CAs (DHS, NASA, OCIO, SSA)
09/04/2015	5.2	Added content for Raytheon SHA-256 PKI
11/13/2015	5.3	Added content for DoD [ID | SW] [EMAIL] CAs 33-38 and ORC ECA 6. Removed content for Cassidian/Airbus (decommissioned)
12/04/2015	5.4	Added content for DoD [ID] [EMAIL] CAs 39-44
01/12/2016	5.5	Added content for Carillon Federal Services PKI Removed expired content for DoD [EMAIL] CA 25-26
01/26/2016	5.6	Added content for re-keyed Entrust SSP PKI chain
03/16/2016	5.7	Added content for DoD ID SW CAs 45-46 and IndenTrust NFI (IdenTrust Root and Booz Allen PIV-I CAs)
04/18/2016	5.8	Added content for DoD Root CA 4, DoD ID SW CAs 47-48, and IndenTrust ECA 5. Updated Lockheed Martin Assurance Level section.
05/18/2016	5.9	Added content for Lockheed Martin SHA-256, CSRA (Symantec NFI), Treasury Fiscal Service Issuing CA (re-keyed), IdenTrust ECA S21, and ORC NFI 3. Removed expired Treasury Fiscal Service Issuing CA. Added TSCP SHA-256 Assurance Levels.

Table of Contents

1.0 Introduction

This document provides Certification Authority (CA) certificate trust chain and assurance level information for all Department of Defense (DoD) approved Public Key Infrastructures (PKIs). DoD Chief Information Officer (CIO) is the governing authority for DoD approved external PKIs. Prior to 2008, the only DoD approved external PKI was the DoD-managed External Certification Authority (ECA) program PKI. On May 24, 2011, DoD CIO released Department of Defense Instruction (DoDI) 8520.02 authorizing PKI interoperability with DoD approved external PKIs The DoD External Interoperability Plan describes the criteria and process for DoD approved external PKIs and is available on the DoD authoritative external Interoperability site http://iase.disa.mil/pki-pke/interoperability/Pages/index.aspx. DoD approved PKIs must conform to all criteria stated in the DoD External Interoperability Plan to include cross certification with the Federal PKI (FPKI) at Federal Bridge Certification Authority (FBCA) medium hardware assurance level or higher and successful completion of Joint Interoperability Test Command (JITC) testing[1]. DoD organizations that wish to interoperate with DoD approved external PKIs must comply with DoD Instruction 8520.02.[2] DoD relying parties may interoperate using cross-certificate trust or direct trust. If interoperating using direct trust, DoD relying parties must ensure that they are only accepting PKI credentials that meet the FBCA medium hardware assurance level restriction.[3] In addition to PKI authentication and validation, administrators should ensure that DoD information systems are performing access control.[4]

[1] The DoD Partner PKI Interoperability test plan is located on the external interoperability site at http://iase.disa.mil/pki-pke/interoperability/Pages/index.aspx

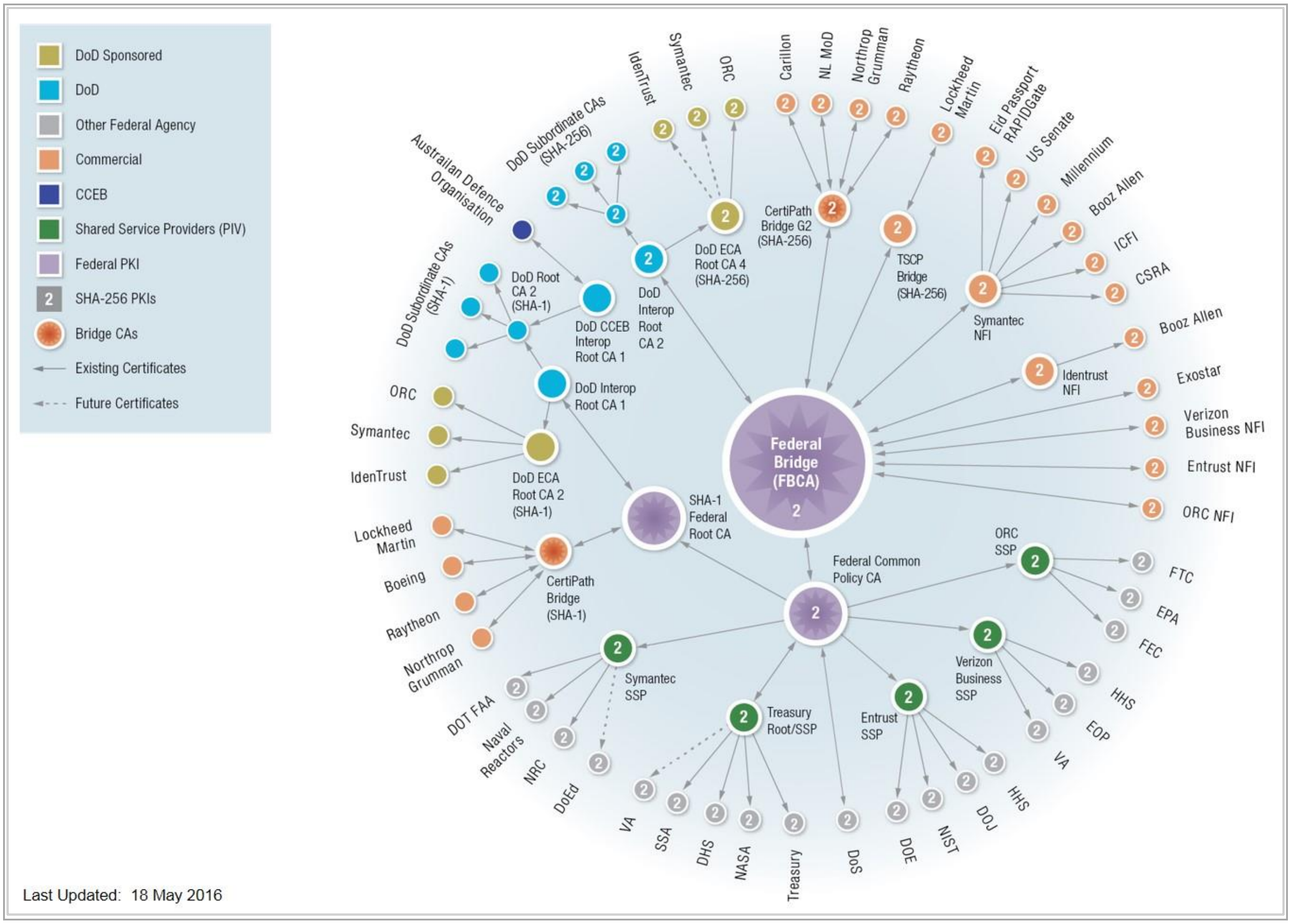
[2] DoD 8520.02 is available at http://www.dtic.mil/whs/directives/corres/pdf/852002p.pdf

[3] For more information on Assurance Levels, see Section 6.

[4] DoD CIO Memorandum, "Compliance and Review of Logical Access Control in Department of Defense (DoD) Processes is available at http://www.doncio.navy.mil/uploads/0205OPP64355.pdf

2.0 DoD PKI External Interoperability Landscape

The following diagram provides an overview of the Federal PKI Interoperability Landscape and illustrates the cross-certificate trust relationships between DoD PKI and DoD approved external PKIs:



Last Updated: 18 May 2016

3.0 DoD PKI Trust Chains

DoD PKI began as a medium assurance pilot in 1998 and has since evolved to a heavily operationalized PKI with over 4.5 million subscribers. DoD currently has over 30 issuing CAs that issues both hardware and software certificates at various assurance levels. DoD most commonly distributes CA certificates with the PKE InstallRoot utility.[5] It also has CA certificates which support cross-certificate interoperability with its Federal, industry, and international partners which are not included in the base InstallRoot package.

3.1 *DoD Trust Anchors*

3.1.1 DoD Root CA 2

DoD Root CA 2 is the primary SHA-1 DoD trust anchor for which all DoD end entity and intermediate CA certificates should be validated against. This trust anchor has issued DoD CAs 25-36, 39, 40 and DoD Intermediate CA 1-2.

	TRUST ANCHOR
Issuer	`CN=DoD Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US`
Subject	`CN=DoD Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US`
Serial #	`0x05`
Valid From	`Dec 13 15:00:10 2004 GMT`
Valid To	`Dec  5 15:00:10 2029 GMT`
SHA-1 Print	`8C:94:1B:34:EA:1E:A6:ED:9A:E2:BC:54:CF:68:72:52:B4:C9:B5:61`

3.1.2 DoD Root CA 3

DoD Root CA 3 is the primary SHA-256 DoD trust anchor for which all DoD SHA-256 end entity and intermediate CA certificates should be validated against. This trust anchor will issue SHA-256 issuing CAs. This trust anchor has issued DoD CAs 37-38, 41-46.

	TRUST ANCHOR
Issuer	`CN=DoD Root CA 3,OU=PKI,OU=DoD,O=U.S. Government,C=US`
Subject	`CN=DoD Root CA 3,OU=PKI,OU=DoD,O=U.S. Government,C=US`
Serial #	`0x01`
Valid From	`Mar 20 18:46:41 2012 GMT`
Valid To	`Dec 30 18:46:41 2029 GMT`
SHA-1 Print	`D7:3C:A9:11:02:A2:20:4A:36:45:9E:D3:22:13:B4:67:D7:CE:97:FB`

3.1.3 DoD Root CA 4

DoD Root CA 4 is the primary ECC p256/SHA-256 DoD trust anchor for which all DoD ECC p256/SHA-256 end entity and intermediate CA certificates should be validated against. This trust anchor will issue ECC p256/SHA-256 issuing CAs. This trust anchor has issued DoD CAs 47-48.

	TRUST ANCHOR
Issuer	`CN=DoD Root CA 4,OU=PKI,OU=DoD,O=U.S. Government,C=US`
Subject	`CN=DoD Root CA 4,OU=PKI,OU=DoD,O=U.S. Government,C=US`
Serial #	`0x01`
Valid From	`Jul 30 19:48:23 2012 GMT`
Valid To	`Jul 25 19:48:23 2032 GMT`
SHA-1 Print	`B8:26:9F:25:DB:D9:37:EC:AF:D4:C3:5A:98:38:57:17:23:F2:D0:26`

[5] InstallRoot is available on the IASE PKE site at http://iase.disa.mil/pki-pke/Pages/tools.aspx

3.1.4 DoD Interoperability Root CA 1

DoD Interoperability Root CA 1 is the SHA-1 DoD trust anchor for cross-certificate trust with SHA-1 DoD approved external PKIs.

TRUST ANCHOR	
Issuer	CN=DoD Interoperability Root CA 1,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DoD Interoperability Root CA 1,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x06
Valid From	Jun 20 14:49:11 2007 GMT
Valid To	Jun 15 14:49:11 2027 GMT
SHA-1 Print	0A:34:BE:0A:96:BA:D5:33:55:8D:16:84:2C:38:7D:74:91:0D:AF:12

3.1.5 DoD Interoperability Root CA 2

DoD Interoperability Root CA 2 is the SHA-256 DoD trust anchor for cross-certificate trust with SHA-256 DoD approved external PKIs.

TRUST ANCHOR	
Issuer	CN=DoD Interoperability Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DoD Interoperability Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x01
Valid From	Nov 29 14:25:10 2010 GMT
Valid To	Nov 24 14:25:10 2030 GMT
SHA-1 Print	52:2E:1B:F5:BE:15:2F:A9:8B:ED:4F:01:AA:44:1D:01:09:2D:5A:31

3.1.6 DoD CCEB Interoperability Root CA 1

US DoD CCEB Interoperability Root CA 1 is the SHA-1 DoD trust anchor for cross-certificate trust with the SHA-1 Combined Communications-Electronics Board (CCEB) partner National Defense PKIs. Partner National Defense PKIs include Australian Defence Organisation (ADO), Canada Department of National Defence (DND), New Zealand Defence Force, and the United Kingdom Ministry of Defence (MOD). Since the preferred method of certificate path processing is cross-certificate trust, cross certificate trust chains will be published. Additionally, for applications that do not support cross-certificate trust, the direct trust chains will also be posted. However, application owners that interoperate using direct trust will need to ensure extra precautions are in place to ensure that only certificates with DoD approved PKI certificate policy OIDs are accepted for authentication. Additionally, direct trust application owners will need to remove the CCEB partner PKI trust anchors in the event of a compromise since they will be unable to rely upon a revocation by the DoD. Since CCEB is a Category III PKI, the trust chains will be listed in Section 5.4, *Foreign, Allied, or Coalition Partner PKIs or other PKIs*.

TRUST ANCHOR	
Issuer	CN=US DoD CCEB Interoperability Root CA 1,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=US DoD CCEB Interoperability Root CA 1,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x01
Valid From	Nov 29 17:47:23 2010 GMT
Valid To	Nov 24 17:47:23 2030 GMT
SHA-1 Print	E0:41:0B:4A:58:2F:B1:C4:DD:52:B0:31:2B:A3:F4:39:4D:4F:01:B8

3.2 DoD Intermediate and Subordinate/Issuing CAs

DoD Intermediate and Subordinate CA certificates are a part of the PKE InstallRoot utility. Additionally, they are hosted in Global Directory Service (GDS).[6]

3.2.1 DoD RSA2048/SHA-1 Subordinate CAs

	ISSUING CA
Issuer	CN=DoD Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD CA-27,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x01B2
Valid From	Sep 8 15:50:25 2011 GMT
Valid To	Sep 8 15:50:25 2017 GMT
SHA-1	CE:D0:0D:53:66:8B:58:7E:7B:6B:A6:E1:3C:05:1D:1B:59:C2:5E:6B

	ISSUING CA
Issuer	CN=DoD Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD EMAIL CA-27,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x01B6
Valid From	Sep 8 16:00:18 2011 GMT
Valid To	Sep 8 16:00:18 2017 GMT
SHA-1 Print	6F:EE:67:34:5F:F6:26:5F:13:37:00:AC:00:1A:51:F0:01:3B:47:7D

	ISSUING CA
Issuer	CN=DoD Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD CA-28,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x01B3
Valid From	Sep 8 15:57:01 2011 GMT
Valid To	Sep 8 15:57:01 2017 GMT
SHA-1 Print	F0:26:B3:B7:86:6E:4D:EC:FE:5C:3E:C1:5C:60:AC:6C:A1:24:61:1C

	ISSUING CA
Issuer	CN=DoD Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD EMAIL CA-28,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x01B7
Valid From	Sep 8 16:01:19 2011 GMT
Valid To	Sep 8 16:01:19 2017 GMT
SHA-1 Print	38:CA:D5:1F:D6:03:E4:50:BC:66:CD:8B:C1:52:FB:CE:35:44:C7:A4

	ISSUING CA
Issuer	CN=DoD Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD CA-29,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x01B4
Valid From	Sep 8 15:58:26 2011 GMT
Valid To	Sep 8 15:58:26 2017 GMT
SHA-1 Print	4E:9B:43:6D:B4:F0:90:AD:3D:9E:6E:00:AE:DF:44:48:1C:AA:B7:6F

	ISSUING CA
Issuer	CN=DoD Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD EMAIL CA-29,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x01B8
Valid From	Sep 8 16:02:14 2011 GMT
Valid To	Sep 8 16:02:14 2017 GMT
SHA-1 Print	81:0B:FB:48:C1:AF:A8:E3:C5:FF:7D:50:B3:28:57:6A:5E:BF:9E:29

[6] All DoD Intermediate and Subordinate/Issuing CAs issued from DoD Root CA 2 can be pulled from GDS at http://crl.disa.mil/issuedby/DODROOTCA2_IB.p7c or https://crl.disa.mil

ISSUING CA	
Issuer	CN=DoD Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD CA-30,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x01B5
Valid From	Sep 8 15:59:24 2011 GMT
Valid To	Sep 8 15:59:24 2017 GMT
SHA-1 Print	BC:AB:48:78:BA:72:DC:43:5B:20:86:02:E8:BB:76:9D:08:E1:A9:0E

ISSUING CA	
Issuer	CN=DoD Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD EMAIL CA-30,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x01B9
Valid From	Sep 8 16:03:08 2011 GMT
Valid To	Sep 8 16:03:08 2017 GMT
SHA-1 Print	44:F7:8C:98:37:19:29:1E:CB:87:70:09:40:68:DA:84:1D:AC:85:45

ISSUING CA	
Issuer	CN=DoD Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD CA-31,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x039D
Valid From	Jan 16 14:49:30 2013 GMT
Valid To	Jan 16 14:49:30 2019 GMT
SHA-1 Print	07:A2:9B:87:8A:0D:C9:C3:F9:79:B9:8B:92:E4:0D:DD:33:9C:F0:87

ISSUING CA	
Issuer	CN=DoD Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD EMAIL CA-31,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x039F
Valid From	Jan 16 14:52:43 2013 GMT
Valid To	Jan 16 14:52:43 2019 GMT
SHA-1 Print	8C:41:53:A8:95:CE:01:1A:E1:31:1F:C7:E0:71:4C:BA:86:D7:1A:3E

ISSUING CA	
Issuer	CN=DoD Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD CA-32,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x03A1
Valid From	Feb 4 20:44:05 2013 GMT
Valid To	Feb 4 20:44:05 2019 GMT
SHA-1 Print	2C:3C:9B:8B:2D:9B:D4:29:DF:DE:BB:80:E9:07:E8:A2:E6:A1:AE:40

ISSUING CA	
Issuer	CN=DoD Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD EMAIL CA-32,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x03A2
Valid From	Feb 4 20:48:12 2013 GMT
Valid To	Feb 4 20:48:12 2019 GMT
SHA-1 Print	60:75:8C:59:72:01:93:EB:45:72:5C:AB:34:E8:F8:DE:5C:C5:B5:FD

ISSUING CA	
Issuer	CN=DoD Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD ID CA-33,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x079C
Valid From	Sep 23 13:32:32 2015 GMT
Valid To	Sep 22 13:32:32 2021 GMT
SHA-1 Print	C2:02:48:28:7B:45:71:67:D4:F2:A4:36:63:A9:83:25:3E:B2:9E:84

	ISSUING CA
Issuer	CN=DoD Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD EMAIL CA-33,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x079D
Valid From	Sep 23 13:34:57 2015 GMT
Valid To	Sep 22 13:34:57 2021 GMT
SHA-1 Print	A5:3A:58:85:C1:3C:5B:D4:9D:60:E2:43:0E:6C:E3:13:4C:7F:D9:C1

	ISSUING CA
Issuer	CN=DoD Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD ID CA-34,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x079F
Valid From	Sep 23 13:40:30 2015 GMT
Valid To	Sep 22 13:40:30 2021 GMT
SHA-1 Print	4C:52:90:42:A6:74:FE:F7:67:18:92:3D:8F:78:88:AC:4C:B6:C1:33

	ISSUING CA
Issuer	CN=DoD Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD EMAIL CA-34,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x07A0
Valid From	Sep 23 13:41:54 2015 GMT
Valid To	Sep 22 13:41:54 2021 GMT
SHA-1 Print	38:53:E2:8E:C5:4F:2F:00:8A:53:F9:2C:57:A1:C1:8B:0C:DE:0C:56

	ISSUING CA
Issuer	CN=DoD Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD ID SW CA-35,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x079E
Valid From	Sep 23 13:37:50 2015 GMT
Valid To	Sep 22 13:37:50 2021 GMT
SHA-1 Print	03:61:1D:56:F2:53:D3:9F:DB:51:E1:92:05:4F:A8:CE:30:06:A8:44

	ISSUING CA
Issuer	CN=DoD Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD ID SW CA-36,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x07A1
Valid From	Sep 23 13:44:42 2015 GMT
Valid To	Sep 22 13:44:42 2021 GMT
SHA-1 Print	5B:A6:36:9B:2F:85:4A:7E:96:96:8A:EB:E0:1C:C3:84:45:9B:5C:FD

	ISSUING CA
Issuer	CN=DoD Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD ID CA-39,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x07C3
Valid From	Nov 9 14:21:57 2015 GMT
Valid To	Nov 8 14:21:57 2021 GMT
SHA-1 Print	39:CC:E3:82:DD:33:07:A5:23:2A:33:EA:4F:16:B3:55:FC:F4:D4:6B

	ISSUING CA
Issuer	CN=DoD Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD EMAIL CA-39,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x07C1
Valid From	Nov 9 14:14:47 2015 GMT
Valid To	Nov 8 14:14:47 2021 GMT
SHA-1 Print	E2:0C:A9:37:03:DE:60:B1:20:B9:DB:1B:86:E0:DF:8E:82:F8:58:16

ISSUING CA	
Issuer	CN=DoD Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD ID CA-40,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x07C4
Valid From	Nov 9 14:22:54 2015 GMT
Valid To	Nov 8 14:22:54 2021 GMT
SHA-1 Print	37:24:FD:13:51:73:4A:2D:11:F7:2B:7D:D2:03:A4:F1:D6:8A:63:D2

ISSUING CA	
Issuer	CN=DoD Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD EMAIL CA-40,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x07C2
Valid From	Nov 9 14:18:43 2015 GMT
Valid To	Nov 8 14:18:43 2021 GMT
SHA-1 Print	6F:69:DD:25:2E:13:D8:75:36:BA:AE:71:44:7F:71:54:87:29:39:3F

ISSUING CA	
Issuer	CN=DoD Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DoD Intermediate CA-1,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x2C
Valid From	Feb 5 15:36:43 2008 GMT
Valid To	Feb 4 14:36:43 2018 GMT
SHA-1 Print	50:43:43:5C:89:B7:A7:7D:88:41:37:FE:EF:C0:0D:C7:E2:AB:94:78

ISSUING CA	
Issuer	CN=DoD Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DoD Intermediate CA-2,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x2D
Valid From	May 7 14:44:51 2008 GMT
Valid To	May 7 13:44:51 2018 GMT
SHA-1 Print	77:B6:B9:42:F8:87:60:8B:AD:B8:37:56:4D:9A:ED:85:AE:D6:FC:7D

ISSUING CA	
Issuer	CN=DoD Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD NPE CA-1, ou=PKI, ou=DoD, o=U.S. Government, c=US
Serial #	0x031C
Valid From	Sep 17 13:01:16 2012 GMT
Valid To	Sep 17 13:01:16 2018 GMT
SHA-1 Print	F2:0E:5D:8D:BE:D9:32:AD:35:24:AC:6F:81:36:F0:C8:76:FE:D2:70

ISSUING CA	
Issuer	CN=DoD Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD NPE CA-2, ou=PKI, ou=DoD, o=U.S. Government, c=US
Serial #	0x032B
Valid From	Oct 1 13:32:18 2012 GMT
Valid To	Oct 1 13:32:18 2018 GMT
SHA-1 Print	05:83:6F:FB:EB:A9:74:2B:39:85:8A:87:1F:4C:D1:C2:06:8B:56:53

3.2.2 DoD RSA2048/SHA-256 Subordinate CAs

ISSUING CA	
Issuer	CN=DoD Root CA 3,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD ID SW CA-37,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x12
Valid From	Sep 23 15:23:05 2015 GMT
Valid To	Sep 23 15:23:05 2021 GMT
SHA-1 Print	5E:AE:74:A8:06:8D:42:F2:F3:E0:17:4B:F2:70:A1:3A:92:EA:AA:5D

ISSUING CA	
Issuer	CN=DoD Root CA 3,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD ID SW CA-38,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x13
Valid From	Sep 23 15:24:51 2015 GMT
Valid To	Sep 23 15:24:51 2021 GMT
SHA-1 Print	81:8E:DA:EF:92:57:79:F0:41:93:94:F5:A3:05:FF:CC:46:3D:75:EE

ISSUING CA	
Issuer	CN=DoD Root CA 3,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD ID CA-41,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x18
Valid From	Nov 9 16:13:56 2015 GMT
Valid To	Nov 9 16:13:56 2021 GMT
SHA-1 Print	FE:E5:43:48:3A:C0:AC:B5:19:68:87:15:23:7D:3B:57:B9:D3:47:55

ISSUING CA	
Issuer	CN=DoD Root CA 3,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD EMAIL CA-41,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x14
Valid From	Nov 9 16:05:27 2015 GMT
Valid To	Nov 9 16:05:27 2021 GMT
SHA-1 Print	38:34:49:9D:17:5C:03:C4:B8:EF:E5:2D:D8:B8:BF:03:18:5C:AB:DB

ISSUING CA	
Issuer	CN=DoD Root CA 3,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD ID CA-42,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x19
Valid From	Nov 9 16:15:02 2015 GMT
Valid To	Nov 9 16:15:02 2021 GMT
SHA-1 Print	8B:12:5C:FC:27:16:55:8D:71:6A:9F:87:DB:7C:A8:31:6D:11:23:6E

ISSUING CA	
Issuer	CN=DoD Root CA 3,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD EMAIL CA-42,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x15
Valid From	Nov 9 16:09:42 2015 GMT
Valid To	Nov 9 16:09:42 2021 GMT
SHA-1 Print	C3:AD:7E:15:9F:17:4B:E6:AA:42:AF:83:93:98:0E:98:5B:78:D5:FE

ISSUING CA	
Issuer	CN=DoD Root CA 3,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD ID CA-43,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x1A
Valid From	Nov 9 16:16:01 2015 GMT
Valid To	Nov 9 16:16:01 2021 GMT
SHA-1 Print	98:D3:E3:3B:50:B8:F6:AC:FF:8C:60:20:E2:9F:F9:67:EB:0E:9C:18

ISSUING CA	
Issuer	CN=DoD Root CA 3,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD EMAIL CA-43,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x16
Valid From	Nov 9 16:11:02 2015 GMT
Valid To	Nov 9 16:11:02 2021 GMT
SHA-1 Print	A9:0A:AC:BD:D1:85:68:18:28:A4:CA:A4:69:5D:39:EC:9C:24:59:9F

ISSUING CA	
Issuer	CN=DoD Root CA 3,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD ID CA-44,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x1B
Valid From	Nov 9 16:18:14 2015 GMT
Valid To	Nov 9 16:18:14 2021 GMT
SHA-1 Print	CB:B4:92:C4:E8:A5:2F:02:47:72:BA:4E:53:D4:73:91:B9:8F:CE:F0

ISSUING CA	
Issuer	CN=DoD Root CA 3,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD EMAIL CA-44,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x17
Valid From	Nov 9 16:12:16 2015 GMT
Valid To	Nov 9 16:12:16 2021 GMT
SHA-1 Print	21:00:1F:0B:33:5F:F9:15:91:00:DD:9A:9C:CA:76:1A:E4:97:10:05

ISSUING CA	
Issuer	CN=DoD Root CA 3,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD ID SW CA-45,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x63
Valid From	Mar 8 13:28:56 2016 GMT
Valid To	Mar 9 13:28:56 2022 GMT
SHA-1 Print	9E:50:AA:4D:A2:44:ED:FD:76:43:86:0C:9D:1B:2E:A4:86:50:75:A4

ISSUING CA	
Issuer	CN=DoD Root CA 3,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD ID SW CA-46,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x64
Valid From	Mar 8 14:22:27 2016 GMT
Valid To	Mar 9 14:22:27 2022 GMT
SHA-1 Print	23:B9:87:4F:99:E0:5D:E8:EB:84:C4:1E:C8:00:9F:B4:5B:BD:96:81

3.2.3 DoD ECC p256/SHA-256 Subordinate CAs

ISSUING CA	
Issuer	CN=DoD Root CA 4,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD ID SW CA-47,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x09
Valid From	Apr 12 13:12:43 2016 GMT
Valid To	Apr 13 13:12:43 2022 GMT
SHA-1 Print	11:8E:7B:1F:77:02:2B:E6:74:80:0B:85:04:C1:73:14:B0:D5:61:29

ISSUING CA	
Issuer	CN=DoD Root CA 4,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD ID SW CA-48,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x0A
Valid From	Apr 12 13:19:49 2016 GMT
Valid To	Apr 13 13:19:49 2022 GMT
SHA-1 Print	05:40:15:6F:C2:A8:BF:AD:49:F9:00:63:F5:79:8C:F3:D3:6D:44:EC

4.0 ECA PKI Trust Chains

The DoD sponsored External Certification Authority (ECA) program was the first DoD approved external PKI. Prior to the 2008 CIO memorandum, *Approval of External Public Key Infrastructures,* it was the only means for DoD partners to interoperate with DoD users and servers. The ECA program is managed by the DoD PKI PMO and has four types of certificates and three different assurance levels. The ECA certificates are included in InstallRoot and GDS hosts the ECA CA information to include CA certificates, cross-certificate content, and Certificate Revocation Lists (CRLs). The DoD Robust Certificate Validation Service (RCVS) does not provide Online Certificate Status Protocol (OCSP) responses for ECA certificates. More information can be found on the ECA homepage, http://iase.disa.mil/pki/eca/Pages/index.aspx. DoD users and systems that choose to trust ECA PKI, should implement direct trust by installing the appropriate trust chain into the application or system trust store. Please note that for servers, this provides the capability to authenticate ECA PKI certificates and a separate access control decision to determine need-to-know should be made before providing access to DoD information systems.

4.1 ECA Trust Anchors

4.1.1 ECA Root CA 2

ECA Root CA 2 is the SHA-1 ECA PKI trust anchor. ECA Root CA 2 has a one-way cross-certificate relationship with DoD Interoperability Root CA 1 which is cross certified with the SHA-1 Federal Root CA. This allows DoD partners to validate ECA SHA-1 certificates against their own PKI trust anchors.

TRUST ANCHOR	
Issuer	CN=ECA Root CA 2,OU=ECA,O=U.S. Government,C=US
Subject	CN=ECA Root CA 2,OU=ECA,O=U.S. Government,C=US
Serial #	0x05
Valid From	Apr 4 14:24:49 2008 GMT
Valid To	Mar 30 14:24:49 2028 GMT
SHA-1 Print	C3:13:F9:19:A6:ED:4E:0E:84:51:AF:A9:30:FB:41:9A:20:F1:81:E4

4.1.2 ECA Root CA 4

ECA Root CA 4 is the SHA-256 ECA trust anchor. ECA Root CA 4 has a one-way cross-certificate relationship with DoD Interoperability Root CA 2 which is cross certified with the Federal Bridge CA. This will allow DoD partners to validate ECA SHA-256 certificates against their own PKI trust anchors. .

TRUST ANCHOR	
Issuer	CN=ECA Root CA 4,OU=ECA,O=U.S. Government,C=US
Subject	CN=ECA Root CA 4,OU=ECA,O=U.S. Government,C=US
Serial #	0x01
Valid From	Mar 20 16:13:04 2012 GMT
Valid To	Dec 30 16:13:04 2029 GMT
SHA-1 Print	73:E8:BB:08:E3:37:D6:A5:A6:AE:F9:0C:FF:DD:97:D9:17:6C:B5:82

4.2 ECA Subordinate/Issuing CAs

There are currently three ECA vendors which operate ECA subordinate CAs: IdenTrust, ORC, and Symantec (formerly VeriSign).

4.2.1 ECA SHA-1 Subordinate CAs[7]

ISSUING CA	
Issuer	CN=ECA Root CA 2,OU=ECA,O=U.S. Government,C=US
Subject	CN=IdenTrust ECA 5,OU=Certification Authorities,OU=ECA,O=U.S. Government,C=US
Serial #	0x74
Valid From	Apr 12 14:33:43 2016 GMT
Valid To	Apr 12 14:33:43 2022 GMT
SHA-1 Print	A2:84:71:83:18:94:CD:4B:75:FD:6A:E4:13:59:D6:DE:DA:53:AF:3D

ISSUING CA	
Issuer	CN=ECA Root CA 2,OU=ECA,O=U.S. Government,C=US
Subject	CN=IdenTrust ECA 4,OU=Certification Authorities,OU=ECA,O=U.S. Government,C=US
Serial #	0x15
Valid From	Jan 16 14:35:32 2014 GMT
Valid To	Jan 16 14:35:32 2020 GMT
SHA-1 Print	19:44:65:2D:36:F8:CF:A2:79:C4:74:0D:1D:1D:E1:82:7D:49:4D:B3

ISSUING CA (CRLS ONLY)	
Issuer	CN=ECA Root CA 2,OU=ECA,O=U.S. Government,C=US
Subject	CN=IdenTrust ECA 3,OU=Certification Authorities,OU=ECA,O=U.S. Government,C=US
Serial #	0x0D
Valid From	Mar 30 13:39:23 2011 GMT
Valid To	Mar 28 13:39:23 2017 GMT
SHA-1 Print	40:91:D6:00:A7:41:E3:7F:B3:18:6B:E1:02:14:E2:FE:2C:1F:0F:71

ISSUING CA	
Issuer	CN=ECA Root CA 2,OU=ECA,O=U.S. Government,C=US
Subject	CN=ORC ECA HW 5,OU=Certification Authorities,OU=ECA,O=U.S. Government,C=US
Serial #	0x18
Valid From	May 19 12:45:53 2014 GMT
Valid To	May 18 12:45:53 2020 GMT
SHA-1 Print	F3:D7:4B:5B:F2:AB:DB:18:70:43:FC:C9:A0:73:81:6C:39:14:74:C0

ISSUING CA (CRLS ONLY)	
Issuer	CN=ECA Root CA 2,OU=ECA,O=U.S. Government,C=US
Subject	CN=ORC ECA HW 4,OU=Certification Authorities,OU=ECA,O=U.S. Government,C=US
Serial #	0x0E
Valid From	Jun 1 13:41:30 2011 GMT
Valid To	May 30 13:41:30 2017 GMT
SHA-1 Print	34:52:42:F5:8E:D3:E7:87:7F:20:56:1E:8C:9F:C3:CB:F9:E4:3D:40

ISSUING CA	
Issuer	CN=ECA Root CA 2,OU=ECA,O=U.S. Government,C=US
Subject	CN=ORC ECA SW 5,OU=Certification Authorities,OU=ECA,O=U.S. Government,C=US
Serial #	0x17
Valid From	May 19 12:33:55 2014 GMT
Valid To	May 18 12:33:55 2020 GMT
SHA-1 Print	E4:64:68:51:F0:95:2A:25:22:C6:4B:96:6A:E2:7E:CE:37:68:DD:B3

[7] All issuing CAs off ECA Root CA 2 can also be pulled from http://crl.disa.mil/issuedby/ECAROOTCA2_IB.p7c or https://crl.disa.mil

ISSUING CA (CRLS ONLY)	
Issuer	CN=ECA Root CA 2,OU=ECA,O=U.S. Government,C=US
Subject	CN=ORC ECA SW 4,OU=Certification Authorities,OU=ECA,O=U.S. Government,C=US
Serial #	0x0F
Valid From	Jun 1 13:43:33 2011 GMT
Valid To	May 30 13:43:33 2017 GMT
SHA-1 Print	74:B8:20:94:0D:E0:07:1E:2C:1D:81:41:52:F7:49:80:2E:CE:89:D1
ISSUING CA	
Issuer	CN=ECA Root CA 2,OU=ECA,O=U.S. Government,C=US
Subject	CN=Symantec Client External Certification Authority - G4,OU=Certification Authorities,OU=ECA,O=U.S. Government,C=US
Serial #	0x16
Valid From	Mar 20 14:24:40 2014 GMT
Valid To	Mar 19 14:24:40 2020 GMT
SHA-1 Print	4A:F9:0B:43:0F:FF:B2:35:C2:14:35:14:CF:A0:55:3F:A9:71:38:00

ISSUING CA (CRLS ONLY)	
Issuer	CN=ECA Root CA 2,OU=ECA,O=U.S. Government,C=US
Subject	CN=VeriSign Client External Certification Authority - G3,OU=Certification Authorities,OU=ECA,O=U.S. Government,C=US
Serial #	0x10
Valid From	Jul 6 14:05:39 2011 GMT
Valid To	Jul 4 14:05:39 2017 GMT
SHA-1 Print	3C:7D:56:57:87:67:68:7F:38:24:2E:48:C4:D9:68:66:6F:94:D8:88

4.2.2 ECA SHA-256 Subordinate CAs[8]

ISSUING CA	
Issuer	CN=ECA Root CA 4,OU=ECA,O=U.S. Government,C=US
Subject	CN=ORC ECA 6,OU=Certification Authorities,OU=ECA,O=U.S. Government,C=US
Serial #	0x08
Valid From	Sep 1 13:34:20 2015 GMT
Valid To	Sep 1 13:34:20 2021 GMT
SHA-1 Print	66:6D:13:D6:EF:E8:35:29:31:9E:88:F3:FB:F5:AD:E4:40:D4:A5:DA

ISSUING CA	
Issuer	CN=ECA Root CA 4,OU=ECA,O=U.S. Government,C=US
Subject	CN=IdenTrust ECA S21,OU=Certification Authorities,OU=ECA,O=U.S. Government,C=US
Serial #	0x78
Valid From	May 17 12:18:15 2016 GMT
Valid To	May 18 12:18:15 2022 GMT
SHA-1 Print	1A:57:5B:51:24:E4:54:24:EE:6A:89:17:EE:EC:BC:14:84:0C:6E:57

[8] All issuing CAs off ECA Root CA 4 can also be pulled from http://crl.disa.mil/issuedby/ECAROOTCA4_IB.p7c or https://crl.disa.mil

5.0 DoD Approved External PKI Trust Chains

In addition to the DoD and ECA PKI, the external PKIs listed in this section are approved for use within DoD at the Federal PKI medium hardware assurance level or higher (although many PKIs have multiple assurance levels).[9] Some of the partners listed in this section maintain their own PKI, referred to within the Federal PKI community as "Legacy PKIs", and many obtain their PKI certificates through Shared Service Providers (SSPs) or other commercial Non-Federal Issuers (NFIs).

The DoD External Interoperability Plan (EIP) defines three categories of PKIs:[10]

1. Category I: U.S. Federal agency PKIs
2. Category II: Non-Federal Agency PKIs cross certified with the FBCA or PKIs from other PKI Bridges that are cross certified with the FBCA
3. Category III: Foreign, Allied, or Coalition Partner PKIs or other PKIs

5.1 DoD Approved External PKI Summary

Type	PKI	Highest Assurance Level	Date Tested	Date Retested
DoD Sponsored	**DoD External Certification Authority (ECA) Program**	Medium Hardware	N/A	
Category I	**Entrust SSP PKI** *Agencies include, but are not limited to:*	PIV	Feb-10	Jan-16
	Department of Energy			
	Department of Justice			
	National Institute of Standards and Technology			
	Health and Human Services	PIV	Oct-13	
Category I	**ORC SSP PKI** *Agencies include, but are not limited to:* ***Environmental Protection Agency***	PIV	Dec-08	
Category I	**Department of State PKI**	PIV	Sep-08	
Category I	**Symantec SSP PKI (formerly VeriSign SSP PKI)** *Agencies include, but are not limited to:*	PIV	Nov-08	
	Department of Transportation / Federal Aviation Administration	PIV	Nov-08	
	Naval Reactors	PIV		

[9] See Section 6.0 for more details on assurance levels.

[10] The DoD External Interoperability Plan is available on the DoD authoritative External PKI Interoperability site at http://iase.disa.mil/pki-pke/Documents/unclass-dod_xternal_interop_plan_082010.pdf or on the JITC External PKI site at http://jitc.fhu.disa.mil/pki/documents/dod_external_interoperability_plan_aug_2010.pdf

Type	PKI	Highest Assurance Level	Date Tested	Date Retested
	Nuclear Regulatory Commission	PIV	Apr-15	
Category I	**U.S. Treasury SSP PKI** *Agencies include:*	PIV	Sep-08	
	Department of Homeland Security	PIV	Mar-09	
	Fiscal Service	PIV	Mar-09	
	National Aeronautics and Space Administration	PIV	Mar-09	
	Social Security Administration	PIV	Jan-09	
	U.S. Treasury Department - OCIO	PIV	Sep-08	
	Department of Veteran Affairs	PIV	Pending	
Category I	**Verizon Business SSP PKI** *Agencies include:*	PIV	Oct-09	
	Department of Veteran Affairs	PIV	Oct-09	
	Executive Office of the President	PIV		
	Health and Human Services	PIV		
Category II	**Boeing PKI**	Medium Hardware	May-12	Jun-13
Category II	**Carillon Federal Services PKI**	PIV-I	Dec-15	
Category II	**Entrust Managed Services NFI PKI**	PIV-I	Oct-11	
Category II	**Exostar LLC PKI**	Medium Hardware	Sep-09	Apr-14
Category II	**IdenTrust NFI**	PIV-I	Mar-16	
Category II	**Lockheed Martin PKI**	Medium Hardware	Mar-09	May-16
Category II	**Netherlands Ministry of Defence**	Medium Hardware	Sep-12	
Category II	**Northrop Grumman PKI**	PIV-I	Nov-08	Jan-15
Category II	**ORC NFI PKI**	PIV-I	Mar-12	May-16
Category II	**Raytheon PKI**	Medium Hardware	Mar-09	Aug-15
Category II	**Symantec NFI PKI (formerly VeriSign NFI PKI)** *Organizations include:*	PIV-I	Apr-11	
	Booz Allen Hamilton	PIV-I	Apr-11	Dec-12
	California Prison Health Care Services	Medium Hardware		
	CSRA (formerly Computer Sciences Corporation)	Medium Hardware	Jan-13	May 16
	Eid Passport	PIV-I	Feb-13	Aug-14
	ICF International	PIV-I		
	Millennium Challenge Corporation	PIV-I		
	State of Colorado	Medium Hardware		
	State of Kansas	Medium Hardware		
	U.S. Senate	PIV-I		
Category II	**Verizon Business NFI PKI**	PIV-I	Jul-11	
Category III	**Australian Defence Organisation**	Medium Hardware	Jun-13	Jun-14

5.2 Federal Agencies (Category I PKIs)

Federal Agency PKIs are defined in the DoD External Interoperability Plan as Category I PKIs and must adhere to FIPS 201 and the Personal Identity Verification (PIV) standard.[11] Although the Category I PKIs have PIV certificates, some have other non-PIV certificates at varying assurance levels. All PIV certificates issued after December 31, 2010 must be SHA-256. DoD application owners should ensure their systems are patched or upgraded as applicable to support validation of SHA-256 certificates.

5.2.1 Entrust SSP PKI (GSA MSO)

The General Services Administration Managed Service Office (GSA MSO) provides PIV credentials to a number of Federal agencies as a Shared Service Provider (SSP).[12] The GSA MSO established the USAccess program to offer federal agencies a managed, shared service solution to simplify the process of procuring and maintaining PIV credentials. Currently GSA MSO credentials are provided solely by the Entrust SSP. DoD approved U.S. Federal Agencies that receive certificates from the Entrust SSP PKI include but not limited to Department of Energy, Department of Justice, and National Institute of Standards and Technology. Entrust SSP PKI has two trust chains as shown below[13]. Entrust SSP currently has a one-way cross-certificate relationship with Federal Common Policy CA.

5.2.1.1 SHA-256 Trust Chain 1 – Current

ENTRUST SSP TRUST ANCHOR- KEY UPDATE #2 (CERTS ISSUED 7/23/15-PRESENT)	
Issuer	OU=Entrust Managed Services Root CA,OU=Certification Authorities,O=Entrust,C=US
Subject	OU=Entrust Managed Services Root CA,OU=Certification Authorities,O=Entrust,C=US
Serial #	0x448062F4
Valid From	Jul 23 16:06:36 2015 GMT
Valid To	Jul 23 16:36:36 2025 GMT
SHA-1 Print	59:C3:01:37:60:A6:A9:67:99:F0:6D:95:BE:92:E2:1D:B1:93:89:6F

ENTRUST SSP ISSUING CA-KEY UPDATE #2 (CERTS ISSUED 7/23/15-PRESENT)	
Issuer	OU=Entrust Managed Services Root CA,OU=Certification Authorities,O=Entrust,C=US
Subject	OU=Entrust Managed Services SSP CA,OU=Certification Authorities,O=Entrust,C=US
Serial #	0x448063D5
Valid From	Jul 30 16:37:44 2015 GMT
Valid To	Jul 23 16:36:36 2025 GMT
SHA-1 Print	DE:C0:1B:F4:0C:15:3F:BC:38:BF:2C:A7:66:B0:4F:9D:FB:DA:30:64

[11] Details on FIPS 201 and PIV can be found at http://csrc.nist.gov/groups/SNS/piv/index.html
[12] The full list of GSA MSO agencies can be found here: http://www.fedidcard.gov/statistics.aspx
[13] Entrust SSP maintains production CA information at https://federaladminservices.managed.entrust.com/fedcerts/

5.2.1.2 SHA-256 Trust Chain 2 – CRLs only

ENTRUST SSP TRUST ANCHOR- KEY UPDATE #1	
Issuer	OU=Entrust Managed Services Root CA,OU=Certification Authorities,O=Entrust,C=US
Subject	OU=Entrust Managed Services Root CA,OU=Certification Authorities,O=Entrust,C=US
Serial #	0x447F9CF2
Valid From	May 9 13:32:31 2009 GMT
Valid To	May 9 14:02:31 2019 GMT
SHA-1 Print	69:27:4F:4B:F3:0B:74:BE:27:F7:39:6D:50:AC:46:8D:FE:5F:01:65

ENTRUST SSP ISSUING CA-KEY UPDATE #1	
Issuer	OU=Entrust Managed Services Root CA,OU=Certification Authorities,O=Entrust,C=US
Subject	OU=Entrust Managed Services SSP CA,OU=Certification Authorities,O=Entrust,C=US
Serial #	0x447F9D1F
Valid From	May 9 15:32:06 2009 GMT
Valid To	May 9 14:02:31 2019 GMT
SHA-1 Print	B6:7E:30:BE:F7:4C:37:F9:71:6B:00:BC:DC:5C:85:9F:73:92:59:62

HEALTH AND HUMAN SERVICES INTERMEDIATE CA-	
Issuer	OU=Entrust Managed Services Root CA,OU=Certification Authorities,O=Entrust,C=US
Subject	CN=HHS-FPKI-Intermediate-CA-E1,OU=Certification Authorities,OU=HHS,O=U.S. Government,C=US
Serial #	0x44801668
Valid From	Mar 7 17:41:14 2013 GMT
Valid To	May 9 14:02:31 2019 GMT
SHA-1 Print	35:F9:51:6B:2C:CC:54:95:92:94:58:4E:72:B2:72:EF:CC:A9:65:A3

5.2.1.3 End Entity Information

Entrust SSP PKI issues SHA-256 end entity certificates.

5.2.2 ORC SSP PKI

ORC SSP PKI provides PIV credentials to federal agencies including the DoD approved Environmental Protection Agency. ORC SSP PKI has one SHA-256 trust chain as shown below. ORC SSP PKI has a one-way cross-certificate relationship with a certificate issued from Federal Common Policy CA to ORC SSP 3.

5.2.2.1 SHA-256 Trust Chain – Current

TRUST ANCHOR	
Issuer	CN=Federal Common Policy CA,OU=FPKI,O=U.S. Government,C=US
Subject	CN=Federal Common Policy CA,OU=FPKI,O=U.S. Government,C=US
Serial #	0x0130
Valid From	Dec 1 16:45:27 2010 GMT
Valid To	Dec 1 16:45:27 2030 GMT
SHA-1 Print	90:5F:94:2F:D9:F2:8F:67:9B:37:81:80:FD:4F:84:63:47:F6:45:C1

ISSUING CA	
Issuer	CN=Federal Common Policy CA,OU=FPKI,O=U.S. Government,C=US
Subject	CN=ORC SSP 3,O=ORC PKI,C=US
Serial #	0x02C2
Valid From	Jan 12 00:54:57 2011 GMT
Valid To	Jan 12 00:52:59 2021 GMT
SHA-1 Print	BB:FA:5A:BD:8A:09:D7:3B:E1:FA:30:36:3F:87:40:2F:EC:53:16:F9

5.2.2.2 End Entity Information

ORC SSP PKI issues SHA-256 end entity certificates.

5.2.3 Department of State PKI

The Department of State maintains its own PKI and has one trust anchor with two active issuing CAs: U.S. Department of State AD High Assurance CA (Serial Number: 0x4e331551) which issues user signature and encryption certificates as well as SSL certificates; and U.S. Department of State PIV CA (S/N: 0x40DA5F3D) which issues user PIV authentication certificates. The two active issuing CAs certificates were rolled over; having previously used the following certificates: U.S. Department of State PIV CA (S/N: 0x40DA049D) and U.S. Department of State AD High Assurance CA (S/N: 0x40D9CD13). The Department of State Root CA is two-way cross certified with the Federal Common Policy CA.

5.2.3.1 SHA-256 Trust Chain - Current

DEPARTMENT OF STATE TRUST ANCHOR	
Issuer	`CN=U.S. Department of State AD Root CA,CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,DC=state,DC=sbu`
Subject	`CN=U.S. Department of State AD Root CA,CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,DC=state,DC=sbu`
Serial #	`0x40D9CA01`
Valid From	`Jun 23 17:50:55 2004 GMT`
Valid To	`Jun 23 18:20:55 2034 GMT`
SHA-1 Print	`31:8F:93:37:82:A2:80:88:11:5A:CE:0F:D9:62:EB:EC:8D:3D:EB:FA`

SSL/SIGNATURE/ENCRYPTION ISSUING CA (CURRENT)	
Issuer	`CN=U.S. Department of State AD Root CA,CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,DC=state,DC=sbu`
Subject	`CN=U.S. Department of State AD High Assurance CA,CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,DC=state,DC=sbu`
Serial #	`0x4e331551`
Valid From	`Mar 19 19:03:48 2012 GMT`
Valid To	`Mar 19 19:33:48 2022 GMT`
SHA-1 Print	`35:81:79:8B:77:68:00:A2:B2:BE:F7:F8:B8:36:21:35:AD:8A:7A:E7`

PIV ISSUING CA (CURRENT)	
Issuer	`CN=U.S. Department of State AD Root CA,CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,DC=state,DC=sbu`
Subject	`CN=U.S. Department of State PIV CA,CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,DC=state,DC=sbu`
Serial #	`0x40DA5F3D`
Valid From	`Sep 30 23:18:39 2009 GMT`
Valid To	`Sep 30 23:48:39 2019 GMT`
SHA-1 Print	`1A:48:54:E1:8F:FB:BB:2B:15:82:B8:78:CD:5C:BC:24:2E:4E:30:57`

5.2.3.2 End Entity Information

The Department of State PKI issues SHA-256 end entity certificates.

5.2.4 U.S. Treasury SSP PKI[14][15]

U.S. Treasury operates a SSP PKI which provides PIV credentials to Treasury, Department of Homeland Security, Social Security Administration, and National Aeronautics and Space Administration. Treasury SSP PKI has one Root CA with separate issuing CAs for each agency. All revocation data from each CA is SHA-256. The

[14] U.S. Treasury SSP PKI certificates can be obtained from http://pki.treas.gov/root_sia.p7c

[15] CAs that have been identified as "CRLs only" do not issue new certificates and only issue CRLs. Certificates previously issued from these CAs are still valid.

addition of the SHA-256 issuing CAs occurred at the end of 2010. The U.S. Treasury Root CA is two-way cross certified with Federal Common Policy CA.

5.2.4.1 SHA-256 Trust Chain – Current

TREASURY SSP TRUST ANCHOR – CURRENT	
Issuer	OU=US Treasury Root CA,OU=Certification Authorities,OU=Department of the Treasury,O=U.S. Government,C=US
Subject	OU=US Treasury Root CA,OU=Certification Authorities,OU=Department of the Treasury,O=U.S. Government,C=US
Serial #	0x443EA73A
Valid From	Aug 5 14:16:30 2006 GMT
Valid To	Aug 5 14:46:30 2026 GMT
SHA-1 Print	02:FF:F6:B3:FC:81:5C:57:E6:83:2D:FC:38:61:85:13:33:B0:C3:0B

DHS ISSUING CA – CURRENT	
Issuer	OU=US Treasury Root CA,OU=Certification Authorities,OU=Department of the Treasury,O=U.S. Government,C=US
Subject	OU=DHS CA4,OU=Certification Authorities,OU=Department of Homeland Security,O=U.S. Government,C=US
Serial #	0x4E398128
Valid From	Jun 13 14:35:04 2015 GMT
Valid To	Jun 13 15:05:04 2025 GMT
SHA-1 Print	A3:1A:5D:F2:F1:C1:01:9B:9C:F5:B7:CA:4E:3B:26:65:0B:9C:A9:3F

DHS ISSUING CA – CURRENT	
Issuer	OU=US Treasury Root CA,OU=Certification Authorities,OU=Department of the Treasury,O=U.S. Government,C=US
Subject	OU=DHS CA4,OU=Certification Authorities,OU=Department of Homeland Security,O=U.S. Government,C=US
Serial #	0x4A61D293
Valid From	Jan 21 19:11:28 2011 GMT
Valid To	Jan 21 19:41:28 2021 GMT
SHA-1 Print	49:AE:4F:02:74:19:A3:EB:22:7E:4C:D4:CC:F4:FF:1B:C7:52:13:B6

DHS ISSUING CA (CRLS ONLY)	
Issuer	OU=US Treasury Root CA,OU=Certification Authorities,OU=Department of the Treasury,O=U.S. Government,C=US
Subject	OU=DHS CA4,OU=Certification Authorities,OU=Department of Homeland Security,O=U.S. Government,C=US
Serial #	0x46EACDA1
Valid From	Mar 13 14:53:32 2008 GMT
Valid To	Mar 13 15:23:32 2018 GMT
SHA-1 Print	06:2E:35:55:C2:7A:1F:0B:74:8A:FE:24:5A:8C:E9:A6:C6:C5:77:0D

NASA ISSUING CA – CURRENT	
Issuer	OU=US Treasury Root CA,OU=Certification Authorities,OU=Department of the Treasury,O=U.S. Government,C=US
Subject	OU=NASA Operational CA,OU=Certification Authorities,OU=NASA,O=U.S. Government,C=US
Serial #	0x4E398116
Valid From	Jun 13 14:24:52 2015 GMT
Valid To	Jun 13 14:54:52 2025 GMT
SHA-1 Print	FE:75:72:BB:DE:7B:7F:44:15:2A:CC:8E:17:15:C1:87:14:DC:9D:63

NASA ISSUING CA – CURRENT	
Issuer	OU=US Treasury Root CA,OU=Certification Authorities,OU=Department of the Treasury,O=U.S. Government,C=US
Subject	OU=NASA Operational CA,OU=Certification Authorities,OU=NASA,O=U.S. Government,C=US
Serial #	0x4A61D2A5
Valid From	Jan 22 13:39:06 2011 GMT
Valid To	Jan 22 14:09:06 2021 GMT
SHA-1 Print	76:A6:EA:A8:52:71:0E:00:B3:68:C4:10:80:E6:13:11:40:AA:F1:89

NASA ISSUING CA (CRLS ONLY)	
Issuer	OU=US Treasury Root CA,OU=Certification Authorities,OU=Department of the Treasury,O=U.S. Government,C=US
Subject	OU=NASA Operational CA,OU=Certification Authorities,OU=NASA,O=U.S. Government,C=US
Serial #	0x45F94AB5
Valid From	Mar 15 21:37:07 2007 GMT
Valid To	Mar 15 22:07:07 2017 GMT
SHA-1 Print	F0:8B:32:1E:A8:34:A6:4B:98:68:68:AB:9D:07:05:C8:79:2F:07:AF

NASA ISSUING CA (CRLS ONLY)	
Issuer	OU=US Treasury Root CA,OU=Certification Authorities,OU=Department of the Treasury,O=U.S. Government,C=US
Subject	OU=NASA Operational CA,OU=Certification Authorities,OU=NASA,O=U.S. Government,C=US
Serial #	0x443EA7E9
Valid From	Sep 20 18:41:08 2006 GMT
Valid To	Sep 20 19:11:08 2016 GMT
SHA-1 Print	84:44:CF:42:FC:B8:9B:73:5B:30:BE:CD:8B:A1:A8:B8:50:47:AF:96

TREASURY OCIO ISSUING CA - CURRENT	
Issuer	OU=US Treasury Root CA,OU=Certification Authorities,OU=Department of the Treasury,O=U.S. Government,C=US
Subject	OU=OCIO CA,OU=Certification Authorities,OU=Department of the Treasury,O=U.S. Government,C=US
Serial #	0x4E398101
Valid From	Apr 19 15:17:45 2015 GMT
Valid To	Apr 19 15:47:45 2025 GMT
SHA-1 Print	5A:D2:54:C3:EC:EB:B5:B7:E1:08:CA:A0:CC:80:30:59:8A:7B:77:09

TREASURY OCIO ISSUING CA - CURRENT	
Issuer	OU=US Treasury Root CA,OU=Certification Authorities,OU=Department of the Treasury,O=U.S. Government,C=US
Subject	OU=OCIO CA,OU=Certification Authorities,OU=Department of the Treasury,O=U.S. Government,C=US
Serial #	0x4A61D192
Valid From	Nov 7 14:46:08 2010 GMT
Valid To	Nov 7 15:16:08 2020 GMT
SHA-1 Print	91:8A:68:D8:7F:B6:01:1A:FE:36:66:07:63:19:ED:04:62:DF:09:40

TREASURY OCIO ISSUING CA (CRLS ONLY)	
Issuer	OU=US Treasury Root CA,OU=Certification Authorities,OU=Department of the Treasury,O=U.S. Government,C=US
Subject	OU=OCIO CA,OU=Certification Authorities,OU=Department of the Treasury,O=U.S. Government,C=US
Serial #	0x4A61D147
Valid From	Sep 12 14:46:41 2010 GMT
Valid To	Sep 12 15:16:41 2020 GMT
SHA-1 Print	F9:29:97:90:EB:27:11:25:FD:91:E6:61:CE:DE:4E:E2:02:D7:E7:58

SSA ISSUING CA - CURRENT	
Issuer	OU=US Treasury Root CA,OU=Certification Authorities,OU=Department of the Treasury,O=U.S. Government,C=US
Subject	OU=Social Security Administration Certification Authority,OU=SSA,O=U.S. Government,C=US
Serial #	0x4E3980EF
Valid From	Apr 19 15:04:29 2015 GMT
Valid To	Apr 19 15:34:29 2025 GMT
SHA-1 Print	BB:6C:62:E6:48:D5:03:F1:BE:AB:75:EF:5F:69:B1:72:56:17:59:93

SSA ISSUING CA - CURRENT	
Issuer	OU=US Treasury Root CA,OU=Certification Authorities,OU=Department of the Treasury,O=U.S. Government,C=US
Subject	OU=Social Security Administration Certification Authority,OU=SSA,O=U.S. Government,C=US
Serial #	0x4A61D2BA
Valid From	Feb 16 23:29:58 2011 GMT
Valid To	Feb 16 23:59:58 2021 GMT
SHA-1 Print	B4:B2:09:AA:DE:83:08:34:C9:B5:C2:F8:15:02:1D:28:DC:38:1F:E1

SSA ISSUING CA (CRLS ONLY)	
Issuer	OU=US Treasury Root CA,OU=Certification Authorities,OU=Department of the Treasury,O=U.S. Government,C=US
Subject	OU=Social Security Administration Certification Authority,OU=SSA,O=U.S. Government,C=US
Serial #	0x45F94AA3
Valid From	Mar 15 15:36:50 2007 GMT
Valid To	Mar 15 16:06:50 2017 GMT
SHA-1 Print	70:7C:F3:73:50:83:56:17:47:A2:B9:AA:04:0B:11:DF:F8:DD:A5:79

TREASURY PUBLIC ISSUING CA - CURRENT	
Issuer	OU=US Treasury Root CA,OU=Certification Authorities,OU=Department of the Treasury,O=U.S. Government,C=US
Subject	OU=US Treasury Public CA,OU=Certification Authorities,OU=Department of the Treasury,O=U.S. Government,C=US
Serial #	0x4A61D1DB
Valid From	Dec 5 18:52:36 2010 GMT
Valid To	Dec 5 19:22:36 2020 GMT
SHA-1 Print	14:D4:45:41:52:A6:A1:38:40:52:18:6A:DB:B9:44:FB:2E:1A:76:8D

TREASURY FISCAL SERVICE ISSUING CA – CURRENT	
Issuer	OU=US Treasury Root CA,OU=Certification Authorities,OU=Department of the Treasury,O=U.S. Government,C=US
Subject	OU=Fiscal Service,OU=Department of the Treasury,O=U.S. Government,C=US
Serial #	0x4E398167
Valid From	Oct 17 13:37:26 2015 GMT
Valid To	Oct 17 14:07:26 2025 GMT
SHA-1 Print	ED:3F:B3:16:11:82:57:A4:4E:A1:1A:49:3D:A1:41:5B:EB:30:12:D7

TREASURY FISCAL SERVICE ISSUING CA – CURRENT	
Issuer	OU=US Treasury Root CA,OU=Certification Authorities,OU=Department of the Treasury,O=U.S. Government,C=US
Subject	OU=Fiscal Service,OU=Department of the Treasury,O=U.S. Government,C=US
Serial #	0x4A61D1C9
Valid From	Dec 5 13:38:40 2010 GMT
Valid To	Dec 5 14:08:40 2020 GMT
SHA-1 Print	B3:B9:0E:DE:68:B0:5F:00:96:F5:AA:49:77:87:F9:50:FD:D8:CC:AD

TREASURY FISCAL SERVICE ISSUING CA (CRLS ONLY)	
Issuer	OU=US Treasury Root CA,OU=Certification Authorities,OU=Department of the Treasury,O=U.S. Government,C=US
Subject	OU=Fiscal Service,OU=Department of the Treasury,O=U.S. Government,C=US
Serial #	0x4A61D01A
Valid From	Jul 19 13:43:51 2009 GMT
Valid To	Jul 19 14:13:51 2019 GMT
SHA-1 Print	70:F6:B2:81:9A:37:1F:D4:64:C0:E4:01:93:52:D8:BD:EA:C0:79:8A

TREASURY FISCAL SERVICE ISSUING CA (CRLS ONLY)	
Issuer	OU=US Treasury Root CA,OU=Certification Authorities,OU=Department of the Treasury,O=U.S. Government,C=US
Subject	OU=Fiscal Service,OU=Department of the Treasury,O=U.S. Government,C=US
Serial #	0x46EACEA1
Valid From	Jan 18 14:18:31 2009 GMT
Valid To	Jan 18 14:48:31 2019 GMT
SHA-1 Print	72:2E:ED:EC:5A:B9:F5:18:6D:F7:5B:95:B7:84:87:A7:99:3B:7A:BB

5.2.4.2 End Entity Information

U.S. Treasury SSP PKI issues SHA-256 end entity certificates.

5.2.5 Symantec SSP PKI (formerly VeriSign SSP PKI)

Symantec SSP PKI provides SHA-256 Personal Identity Verification (PIV) credentials to Federal agencies. DoD approved Federal agencies that receive credentials from the Symantec SSP PKI are the Department of Transportation/Federal Aviation Administration and the Department of Energy Naval Reactors. Symantec SSP has one SHA-256 trust chain as shown below. Each trust chain shares a Root and Intermediate CA with different issuing CAs for each agency. Symantec SSP PKI also has device Issuing CA certificates which are currently not included because they don't meet the medium hardware assurance level requirement.

Symantec SSP SHA-2 PKI is subordinate to Federal Common Policy CA which has a two-way cross-certificate with FBCA and several legacy PKIs. Federal Common Policy is also the trust anchor for the other SSPs.

5.2.5.1 Symantec SSP SHA-256 Trust Chain - Current

TRUST ANCHOR	
Issuer	CN=Federal Common Policy CA,OU=FPKI,O=U.S. Government,C=US
Subject	CN=Federal Common Policy CA,OU=FPKI,O=U.S. Government,C=US
Serial #	0x0130
Valid From	Dec 1 16:45:27 2010 GMT
Valid To	Dec 1 16:45:27 2030 GMT
SHA-1 Print	90:5F:94:2F:D9:F2:8F:67:9B:37:81:80:FD:4F:84:63:47:F6:45:C1

INTERMEDIATE CA	
Issuer	CN=Federal Common Policy CA,OU=FPKI,O=U.S. Government,C=US
Subject	CN=VeriSign SSP Intermediate CA - G3,O=VeriSign, Inc.,C=US
Serial #	0x0196
Valid From	Dec 9 19:11:52 2010 GMT
Valid To	Dec 9 19:10:21 2020 GMT
SHA-1 Print	E9:C8:71:5B:87:1D:B1:D8:7B:B6:5B:A2:A5:BB:FA:80:00:DF:78:61

TRANSPORTATION ISSUING CA (USER CERTIFICATES ONLY)	
Issuer	CN=VeriSign SSP Intermediate CA - G3,O=VeriSign, Inc.,C=US
Subject	CN=U.S. Department of Transportation SSP Agency CA G3,OU=U.S. Department of Transportation,O=U.S. Government,C=US
Serial #	0x5FFE0ACFA12B6147F3275B2BBAD93FFF
Valid From	Dec 10 00:00:00 2010 GMT
Valid To	Dec 9 23:59:59 2017 GMT
SHA-1 Print	D2:F1:45:78:99:30:1C:FD:5A:73:D5:AB:27:BA:87:C3:92:85:E7:C3

NAVAL REACTORS ISSUING CA (USER CERTIFICATES ONLY)	
Issuer	CN=VeriSign SSP Intermediate CA - G3,O=VeriSign, Inc.,C=US
Subject	CN=Naval Reactors SSP Agency CA G2,OU=U.S. Department of Energy,O=U.S. Government,C=US
Serial #	0x27B128BB46171BE1C10BB00FDEC27219
Valid From	Dec 10 00:00:00 2010 GMT
Valid To	Dec 9 23:59:59 2017 GMT
SHA-1 Print	93:94:09:F0:4F:CB:2B:EB:71:9D:D2:DF:18:A4:B8:EC:6C:7E:65:A3

NUCLEAR REGULATORY COMMISSION ISSUING CA (USER CERTIFICATES ONLY)	
Issuer	CN=VeriSign SSP Intermediate CA - G3,O=VeriSign\, Inc.,C=US
Subject	CN=NRC SSP Agency CA G2,OU=U.S. Nuclear Regulatory Commission,O=U.S. Government,C=US
Serial #	0x312C238615EF33B963936445ACC9EC4E
Valid From	May 12 00:00:00 2011 GMT
Valid To	May 11 23:59:59 2018 GMT
SHA-1 Print	5F:54:9C:AC:60:C0:57:CB:69:A1:7E:D1:A9:3E:8B:CF:DE:25:D5:BD

5.2.5.2 End Entity Information

Symantec SSP PKI issues SHA-256 end entity certificates.

5.2.6 Verizon Business SSP PKI

Verizon Business SSP PKI provides PIV credentials to federal agencies. DoD approved federal agencies that receive credentials from the Verizon Business SSP PKI are the Department of Veteran Affairs, Executive Office of the President, and Health and Human Services. Verizon Business SSP PKI has one trust chain as shown below. Verizon Business has the same Root and intermediate CA with separate issuing CAs for each agency. DoD relying parties who interoperate with Verizon Business SSP PKI certificates must ensure they can support SHA-256. Verizon Business PKI is subordinate to Federal Common Policy CA which has a two-way cross-certificate with FBCA and several legacy PKIs.

5.2.6.1 SHA-256 Trust Chain - Current

TRUST ANCHOR	
Issuer	CN=Federal Common Policy CA,OU=FPKI,O=U.S. Government,C=US
Subject	CN=Federal Common Policy CA,OU=FPKI,O=U.S. Government,C=US
Serial #	0x0130
Valid From	Dec 1 16:45:27 2010 GMT
Valid To	Dec 1 16:45:27 2030 GMT
SHA-1 Print	90:5F:94:2F:D9:F2:8F:67:9B:37:81:80:FD:4F:84:63:47:F6:45:C1

INTERMEDIATE CA	
Issuer	CN=Federal Common Policy CA,OU=FPKI,O=U.S. Government,C=US
Subject	CN=Betrusted Production SSP CA A1,OU=Betrusted Production SSP CA A1,OU=SSP,O=Betrusted US Inc,C=US
Serial #	0x019A
Valid From	Dec 9 19:55:24 2010 GMT
Valid To	Dec 9 19:49:04 2020 GMT
SHA-1 Print	06:01:BB:DA:D5:A2:82:31:BC:94:36:75:0B:4F:3A:48:4B:AB:06:C3

VETERAN AFFAIRS ISSUING CA	
Issuer	CN=Betrusted Production SSP CA A1,OU=Betrusted Production SSP CA A1,OU=SSP,O=Betrusted US Inc,C=US
Subject	CN=Veterans Affairs User CA B1,OU=PKI,OU=Services,DC=va,DC=gov
Serial #	0x1C5E
Valid From	Aug 7 15:08:04 2008 GMT
Valid To	Aug 7 15:04:49 2018 GMT
SHA-1 Print	7B:D3:F4:8D:67:D4:8D:52:C0:D0:B2:6F:E7:3C:B5:5A:E4:A6:38:0D

EXECUTIVE OFFICE OF THE PRESIDENT SHA-1 ISSUING CA	
Issuer	CN=Betrusted Production SSP CA A1,OU=Betrusted Production SSP CA A1,OU=SSP,O=Betrusted US Inc,C=US
Subject	CN=Executive Office of the President CA-B4,OU=PKI,OU=Services,DC=ssp,DC=eop,DC=gov
Serial #	0x204A
Valid From	Oct 8 16:12:11 2008 GMT
Valid To	Oct 8 16:09:17 2018 GMT
SHA-1 Print	4B:80:C4:9F:B0:7C:FC:74:62:C2:1C:09:0C:34:A8:A8:C3:83:AA:FB

EXECUTIVE OFFICE OF THE PRESIDENT SHA-256 ISSUING CA	
Issuer	CN=Betrusted Production SSP CA A1,OU=Betrusted Production SSP CA A1,OU=SSP,O=Betrusted US Inc,C=US
Subject	CN=Executive Office of the President CA-B8,OU=PKI,OU=Services,DC=ssp,DC=eop,DC=gov
Serial #	0x49FC
Valid From	Jan 25 15:44:57 2011 GMT
Valid To	Jan 25 15:43:46 2021 GMT
SHA-1 Print	A5:41:6C:D5:80:E3:05:DB:C7:65:97:01:BA:8B:F3:9A:41:A1:C9:AA

HEALTH AND HUMAN SERVICES ISSUING CA	
Issuer	CN=Betrusted Production SSP CA A1,OU=Betrusted Production SSP CA A1,OU=SSP,O=Betrusted US Inc,C=US
Subject	CN=HHS-SSP-CA-B7,OU=HHS,O=U.S. Government,C=US,DC=hhs,DC=gov
Serial #	0x0E2B
Valid From	Jul 6 16:07:08 2007 GMT
Valid To	Jul 6 16:05:18 2017 GMT
SHA-1 Print	2F:90:08:7B:96:F7:EC:4A:4C:91:19:5C:64:98:A6:FB:F7:C5:E7:3B

5.2.6.2 End Entity Information

Verizon Business SSP PKI issues SHA-256 end entity certificates.

5.3 Industry Partners (Category II PKIs)

Industry Partners are classified in the DoD External Interoperability Plan as Category II PKIs and in addition to meeting the technical requirements and successfully completing JITC testing, must sign a Memorandum of Agreement (MOA), and be sponsored by a DoD relying party. Industry partners can be approved at PIV-I or Medium Hardware and often have additional assurance levels.[16] PIV-I certificates must be SHA-256. Application owners that need to validate PIV-I certificates should ensure that their applications are patched or upgraded as necessary to be able to validate SHA-256 signed certificates.

5.3.1 Boeing PKI

Boeing PKI is an Aero Defense partner through CertiPath. They currently have a SHA-1 only infrastructure but will be adding a SHA-256 infrastructure at a later date (no timeframe has been announced). The Boeing Root CA currently has a two-way cross-certificate relationship with the SHA-1 CertiPath Bridge CA. The SHA-1 CertiPath Bridge CA has a two-way cross-certificate relationship with the SHA-1 Federal Root CA.

[16] For more information on assurance levels, see Section 6.0.

5.3.1.1 SHA-1 Trust Chain - Current

TRUST ANCHOR	
Issuer	CN=Boeing PCA G2,OU=certservers,O=Boeing,C=US
Subject	CN=Boeing PCA G2,OU=certservers,O=Boeing,C=US
Serial #	0x1CAF04E33ED4A2A745EE302C64D206EC
Valid From	Jan 21 17:52:52 2012 GMT
Valid To	Sep 21 17:58:13 2029 GMT
SHA-1 Print	C9:59:F3:41:30:A7:74:A7:8F:DA:09:97:90:39:4B:A2:5B:BB:79:37

ISSUING CA	
Issuer	CN=Boeing PCA G2,OU=certservers,O=Boeing,C=US
Subject	CN=Boeing SecureBadge Medium G2,OU=certservers,O=Boeing,C=US
Serial #	0x611EEB9600000000006
Valid From	Feb 3 20:17:02 2012 GMT
Valid To	Feb 3 20:27:02 2019 GMT
SHA-1 Print	44:43:2B:B6:29:E1:D7:81:A9:99:F3:88:24:FC:32:5C:D1:C8:9F:78

5.3.1.2 End Entity Information

Boeing currently issues SHA-1 end entity certificates.

5.3.2 Carillon Federal Services PKI

Carillon Federal Services PKI issues PIV-I credentials to Federal, State & Local Agencies as well as private companies that provide products and services to the DoD. The PKI has one SHA-256 Trust Chain as shown below. The Root CA has a two-way trust relationship with the Federal Bridge CA as mapped through the CertiPath Bridge CA-G2 (SHA-256). DoD relying parties that wish to interoperate with Carillon should ensure their applications support SHA-256.

5.3.2.1 SHA-256 Trust Chain – Current

TRUST ANCHOR	
Issuer	CN=Carillon Federal Services NFI Root CA1,OU=Certification Authorities,O=Carillon Federal Services Inc.,C=US
Subject	CN=Carillon Federal Services NFI Root CA1,OU=Certification Authorities,O=Carillon Federal Services Inc.,C=US
Serial #	0x014325B6A074
Valid From	Jun 12 18:46:31 2015 GMT
Valid To	Jun 12 18:46:31 2035 GMT
SHA-1 Print	55:E9:A9:43:49:CD:45:19:0D:C0:FE:ED:B2:2C:B7:C9:71:5C:28:98

ISSUING CA	
Issuer	CN=Carillon Federal Services NFI Root CA1,OU=Certification Authorities,O=Carillon Federal Services Inc.,C=US
Subject	CN=Carillon Federal Services PIV-I CA1,OU=Certification Authorities,O=Carillon Federal Services Inc.,C=US
Serial #	0x0BB34DC334FF
Valid From	Jun 12 19:01:13 2015 GMT
Valid To	Jun 12 19:01:13 2028 GMT
SHA-1 Print	DC:78:C9:7B:02:19:E4:9F:93:81:33:44:5E:18:2D:FA:AC:7C:C8:76

5.3.2.2 End Entity Information

Carillon issues SHA-256 end entity certificates.

5.3.3 Entrust Managed Services NFI PKI

Entrust Managed Services NFI PKI issues PIV-I credentials to non-DoD entities and personnel desiring to use those certificates to interact with DoD Relying Parties. Entrust NFI PKI has one SHA-256 Trust Chain as shown below. The issuing CA also has a two-way cross-certificate relationship with the Federal Bridge CA. DoD relying parties that wish to interoperate with Entrust NFI PKI should ensure their applications support SHA-256.

5.3.3.1 SHA-256 Trust Chain - Current

TRUST ANCHOR	
Issuer	OU=Entrust Managed Services NFI Root CA,OU=Certification Authorities,O=Entrust,C=US
Subject	OU=Entrust Managed Services NFI Root CA,OU=Certification Authorities,O=Entrust,C=US
Serial #	0x4AA7C26D
Valid From	Sep 9 14:27:51 2009 GMT
Valid To	Sep 9 14:57:51 2019 GMT
SHA-1 Print	83:CC:EA:42:6D:45:F7:A4:31:D7:B4:D0:B9:A6:FC:9C:C2:CC:A6:60

ISSUING CA	
Issuer	OU=Entrust Managed Services NFI Root CA,OU=Certification Authorities,O=Entrust,C=US
Subject	OU=Entrust NFI Medium Assurance SSP CA,OU=Certification Authorities,O=Entrust,C=US
Serial #	0x4AA7F719
Valid From	May 23 22:22:23 2011 GMT
Valid To	Aug 23 22:52:23 2019 GMT
SHA-1 Print	73:CA:3C:6D:19:80:1D:D5:AB:88:C8:D0:58:0B:34:DE:82:32:16:41

5.3.3.2 End Entity Information

Entrust NFI PKI issues SHA-256 end entity certificates.

5.3.4 Exostar, LLC.

Exostar, LLC PKI is a SHA-256 Federal Bridge partner. Exostar Federated Identity Service Root CA 2 currently has a two-way cross-certificate relationship with the SHA-256 Federal Bridge CA. Exostar has one SHA-256 trust chain as shown below.

5.3.4.1 SHA-256 Trust Chain – Current

TRUST ANCHOR	
Issuer	CN=Exostar Federated Identity Service Root CA 2,OU=Certification Authorities,O=Exostar LLC,C=US
Subject	CN=Exostar Federated Identity Service Root CA 2,OU=Certification Authorities,O=Exostar LLC,C=US
Serial #	0x315A18EF287EEE924ED386C42DB24B17
Valid From	Jan 25 15:23:41 2013 GMT
Valid To	Jan 25 15:30:19 2030 GMT
SHA-1 Print	C6:B4:F6:D0:B8:6E:EE:2C:02:96:0C:EA:8A:F4:29:37:E8:66:87:EC

ISSUING CA 1	
Issuer	CN=Exostar Federated Identity Service Root CA 2,OU=Certification Authorities,O=Exostar LLC,C=US
Subject	CN=Exostar Federated Identity Service Signing CA 3,DC=evincible,DC=com
Serial #	0x2E0000000292A6E5517B158B23000000000002
Valid From	Apr 9 16:31:10 2014 GMT
Valid To	Apr 9 16:31:10 2024 GMT
SHA-1 Print	F2:42:5B:9A:2F:50:E3:DA:04:42:0D:88:4F:B7:6B:EF:BE:B3:04:15

5.3.4.2 End Entity Information

Exostar currently issues SHA-1 end entity certificates only.

5.3.5 IdenTrust NFI PKI

The IdenTrust Global Common PKI (IdenTrust NFI) issues PIV-I credentials to U.S. Federal agencies, contractors and other entities requiring U.S. Federal reliance or interoperability. IdenTrust Global Common Root CA 1 currently has a two-way cross-certificate relationship with the SHA-256 Federal Bridge CA. IdenTrust NFI has one SHA-256 trust chain as shown below.

5.3.5.1 SHA-256 Trust Chain – Current

	TRUST ANCHOR
Issuer	CN=IdenTrust Global Common Root CA 1,O=IdenTrust,C=US
Subject	CN=IdenTrust Global Common Root CA 1,O=IdenTrust,C=US
Serial #	0x0A0142800000014523CD7FD000000002
Valid From	Jan 16 18:05:05 2014 GMT
Valid To	Jan 16 18:05:05 2034 GMT
SHA-1 Print	AD:00:62:E2:90:97:D8:AA:FE:5B:47:CA:62:B3:57:D9:88:32:E6:A6

	ISSUING CA 1
Issuer	CN=IdenTrust Global Common Root CA 1,O=IdenTrust,C=US
Subject	CN=Booz Allen Hamilton PIVi CA 01,OU=IdenTrust Global Common,O=IdenTrust,C=US
Serial #	0x14A35B824AF8D58C710CCB3D8FEA0CA8
Valid From	Aug 28 17:16:27 2015 GMT
Valid To	Aug 28 17:16:27 2025 GMT
SHA-1 Print	5C:EE:B1:8E:44:50:75:05:9A:00:BB:CC:B4:FB:D1:67:73:7B:69:37

5.3.5.2 End Entity Information

IdenTrust NFI PKI currently issues SHA-256 end entity certificates.

5.3.6 Lockheed Martin

Lockheed Martin PKI is an Aero Defense partner PKI. Lockheed currently has a SHA-1 and SHA-256 infrastructures. Lockheed Martin currently has a two-way cross-certificate relationship with the SHA-1 CertiPath Bridge CA and a two-way cross-certificate relationship with the TSCP SHA-256 Bridge. The SHA-1 CertiPath Bridge CA has a two-way cross-certificate relationship with the SHA-1 Federal Root CA. The TSCP SHA-256 Bridge has a two-way cross-certificate relationship with the FBCA.

5.3.6.1 SHA-1 Trust Chain - Current

	TRUST ANCHOR
Issuer	CN=Lockheed Martin Root Certification Authority,OU=Certification Authorities,O=Lockheed Martin Corporation,L=Denver,ST=Colorado,C=US
Subject	CN=Lockheed Martin Root Certification Authority,OU=Certification Authorities,O=Lockheed Martin Corporation,L=Denver,ST=Colorado,C=US
Serial #	0x13F530A23F6D8EAE437A43064AC60420
Valid From	Jun 8 17:29:09 2006 GMT
Valid To	Nov 15 17:03:39 2026 GMT
SHA-1 Print	E6:DC:D4:3B:E3:9A:88:BB:F2:63:75:59:C6:09:D5:F9:75:A5:2A:37

	ISSUING CA
Issuer	CN=Lockheed Martin Root Certification Authority,OU=Certification Authorities,O=Lockheed Martin Corporation,L=Denver,ST=Colorado,C=US
Subject	CN=Lockheed Martin US Certification Authority-2,OU=Certification Authorities,O=Lockheed Martin Corporation,L=Denver,ST=Colorado,C=US
Serial #	0x6175CFF9000100000006
Valid From	Nov 15 18:48:33 2007 GMT
Valid To	Nov 15 18:58:33 2017 GMT
SHA-1 Print	B0:3A:08:89:94:37:84:F7:63:08:CA:B6:DA:79:76:EE:39:24:90:A5

5.3.6.2 SHA-256 Trust Chain - Current

	TRUST ANCHOR
Issuer	CN=Lockheed Martin Root Certification Authority 2,OU=Certification Authorities,O=Lockheed Martin Corporation,L=Denver,ST=Colorado,C=US
Subject	CN=Lockheed Martin Root Certification Authority 2,OU=Certification Authorities,O=Lockheed Martin Corporation,L=Denver,ST=Colorado,C=US
Serial #	0x7ACE2BC80B3F3791479C8B9E6623875B
Valid From	Jun 19 05:18:34 2013 GMT
Valid To	Jun 19 05:24:38 2030 GMT
SHA-1 Print	C5:FD:5D:D4:37:93:36:07:DE:60:F8:4C:E5:A2:A4:65:21:35:16:18

	ISSUING CA
Issuer	CN=Lockheed Martin Root Certification Authority 2,OU=Certification Authorities,O=Lockheed Martin Corporation,L=Denver,ST=Colorado,C=US
Subject	CN=Lockheed Martin Certification Authority 4 G2,OU=Certification Authorities,O=Lockheed Martin Corporation,C=US
Serial #	0x11489082000000000004
Valid From	Sep 9 23:36:58 2015 GMT
Valid To	Sep 9 23:46:58 2025 GMT
SHA-1 Print	EA:44:FB:F1:CC:3B:5E:24:97:22:86:04:FD:EE:60:4B:F1:85:65:E4

5.3.6.3 End Entity Information

Lockheed currently issues SHA-1 and SHA-256 end entity certificates.

5.3.7 Netherlands Ministry of Defence PKI

The Netherlands Ministry of Defence (NL MoD) operates a PKI to provide defense employees with a capability for secure communications with reliable authentication. It is an implementation of the Dutch Law for electronic signatures and is subordinate to the Dutch government PKI Policy. The NL MoD PKI primarily issues certificates to defense employees and affiliates. Although NL MoD is a foreign PKI, they are considered a Category II PKI since they are a CertiPath Bridge partner. The CertiPath Policy Management Authority (PMA) is responsible for setting, implementing, and administering policy decisions related to the CertiPath Bridge and the related CAs that are cross certified with the CertiPath Bridge.

NL MoD PKI has one SHA-256 Trust Chain as shown below. The NL MoD Intermediate CA has a two-way trust relationship with the Federal Bridge CA as mapped through the CertiPath Bridge CA-G2 (SHA-256). DoD relying parties that wish to interoperate with NL MoD should ensure their applications support SHA-256.

5.3.7.1 SHA-256 Trust Chain – Current

	TRUST ANCHOR
Issuer	CN=Staat der Nederlanden Root CA - G2,O=Staat der Nederlanden,C=NL
Subject	CN=Staat der Nederlanden Root CA - G2,O=Staat der Nederlanden,C=NL
Serial #	0x98968C
Valid From	Mar 26 11:18:17 2008 GMT
Valid To	Mar 25 11:03:10 2020 GMT
SHA-1 Print	59:AF:82:79:91:86:C7:B4:75:07:CB:CF:03:57:46:EB:04:DD:B7:16

	INTERMEDIATE CA
Issuer	CN=Staat der Nederlanden Root CA - G2,O=Staat der Nederlanden,C=NL
Subject	CN=Staat der Nederlanden Organisatie CA - G2,O=Staat der Nederlanden,C=NL
Serial #	0x9896F4
Valid From	Mar 31 12:03:09 2008 GMT
Valid To	Mar 24 13:02:08 2020 GMT
SHA-1 Print	0B:28:99:53:45:31:27:C4:0B:22:FA:95:3D:11:F7:9E:05:2C:05:80

INTERMEDIATE CA	
Issuer	CN=Staat der Nederlanden Organisatie CA - G2,O=Staat der Nederlanden,C=NL
Subject	CN=Ministerie van Defensie Certificatie Autoriteit - G2,O=Ministerie van Defensie,C=NL
Serial #	0x0131354B
Valid From	Nov 10 09:34:25 2010 GMT
Valid To	Mar 23 09:31:44 2020 GMT
SHA-1 Print	B8:4F:18:64:05:75:25:52:09:3D:50:1E:14:8D:27:A8:C2:A3:3E:E3

ISSUING CA	
Issuer	CN=Ministerie van Defensie Certificatie Autoriteit - G2,O=Ministerie van Defensie,C=NL
Subject	CN=Ministerie van Defensie Certificatie Autoriteit Defensiepas - G2,O=Ministerie van Defensie,C=NL
Serial #	0x2E11232C15D59733D1CB7DEF514FE305
Valid From	Nov 16 14:29:29 2010 GMT
Valid To	Mar 22 09:31:00 2020 GMT
SHA-1 Print	66:9E:8B:FC:6B:EC:EC:7C:56:B3:06:9C:C6:2C:38:36:9A:50:22:5F

5.3.7.2 End Entity Information

NL MoD issues SHA-256 end entity certificates.

5.3.8 Northrop Grumman

Northrop Grumman PKI is an Aero Defense partner through CertiPath. Northrop Grumman Corporation Root CAs currently have two-way cross-certificate relationships with the SHA-1 CertiPath Bridge CA for their SHA-1 PKI and a two-way cross-certificate relationship with the SHA-256 CertiPath Bridge CA – G2 for their SHA-256 PKI.

5.3.8.1 SHA-1 Trust Chain - Current

TRUST ANCHOR	
Issuer	CN=Northrop Grumman Corporation Root CA,O=Northrop Grumman Corporation,C=US
Subject	CN=Northrop Grumman Corporation Root CA,O=Northrop Grumman Corporation,C=US
Serial #	0x09ACBF24A21A94B649DD8B86A22D3062
Valid From	Dec 8 18:08:14 2006 GMT
Valid To	Dec 12 20:10:01 2026 GMT
SHA-1 Print	EE:2A:A5:E7:ED:17:03:EF:98:3D:02:B4:9A:59:06:96:49:6F:5B:DD

ISSUING CA	
Issuer	CN=Northrop Grumman Corporation Root CA,O=Northrop Grumman Corporation,C=US
Subject	CN=Northrop Grumman Corporation Issuing CA 2,OU=Northrop Grumman Information Technology,O=Northrop Grumman Corporation,C=US
Serial #	0x6129FFC500010000000E
Valid From	Jun 12 20:28:52 2008 GMT
Valid To	Jun 12 20:38:52 2018 GMT
SHA-1 Print	1A:1C:E7:1D:46:07:E7:A4:0D:BE:6A:B3:5D:FE:DF:7D:76:29:CC:01

5.3.8.2 SHA-256 Trust Chain - Current

TRUST ANCHOR	
Issuer	CN=Northrop Grumman Corporate Root CA-G2,OU=Northrop Grumman Information Technology,O=Northrop Grumman Corporation,C=US
Subject	CN=Northrop Grumman Corporate Root CA-G2,OU=Northrop Grumman Information Technology,O=Northrop Grumman Corporation,C=US
Serial #	0x32ADA9B80CB58EAC43DC76F8AD0C0CFB
Valid From	Oct 11 16:07:09 2013 GMT
Valid To	Oct 11 16:07:09 2033 GMT
SHA-1 Print	41:16:57:F7:83:2C:26:2F:37:3D:8F:9E:09:A1:AF:C4:D0:A1:0A:6A

ISSUING CA	
Issuer	CN=Northrop Grumman Corporate Root CA-G2,OU=Northrop Grumman Information Technology,O=Northrop Grumman Corporation,C=US
Subject	CN=Northrop Grumman Corporate Signing CA-G2,OU=Northrop Grumman Information Technology,O=Northrop Grumman Corporation,C=US
Serial #	0x61848400000000000002
Valid From	Oct 11 18:56:36 2013 GMT
Valid To	Oct 11 19:06:36 2026 GMT
SHA-1 Print	E4:54:AC:18:FC:9A:E0:17:3C:36:5E:87:67:B6:79:CF:E0:36:E6:3F

5.3.8.3 End Entity Information

Northrop currently issues SHA-1 and SHA-256 end entity certificates.

5.3.9 ORC NFI PKI

ORC NFI PKI provides PIV-I credentials to federal agencies, authorized federal contractors, agency-sponsored universities and laboratories, and, if authorized by law, state, local, and tribal governments. ORC NFI PKI has one SHA-256 trust chain as shown below. The ORC NFI Issuing CA has a two-way cross-certificate relationship with the Federal Bridge CA.

5.3.9.1 SHA-256 Trust Chain – Current

TRUST ANCHOR	
Issuer	CN=ORC Root 2,O=ORC PKI,C=US
Subject	CN=ORC Root 2,O=ORC PKI,C=US
Serial #	0x36046D351A45D7AFF0C2E995BFE2969D
Valid From	Dec 13 19:22:00 2010 GMT
Valid To	Dec 13 19:22:00 2035 GMT
SHA-1 Print	A3:29:B4:BE:09:30:70:2A:A6:05:79:B1:56:EC:56:5A:BA:83:63:9C

ISSUING CA	
Issuer	CN=ORC Root 2,O=ORC PKI,C=US
Subject	CN=ORC NFI CA 2,O=ORC PKI,C=US
Serial #	0xEE7CAF3AC34501FD7E415A88A0C4BF51
Valid From	Mar 11 19:54:00 2011 GMT
Valid To	Mar 11 19:56:00 2019 GMT
SHA-1 Print	F4:F9:A3:EC:D9:C8:FA:03:73:A7:28:41:37:F1:D2:CA:AD:2D:D8:34

ISSUING CA	
Issuer	CN=ORC Root 2,O=ORC PKI,C=US
Subject	CN=ORC NFI CA 3,O=ORC PKI,C=US
Serial #	0x1B47BCF310AD545C34FF908742B2AD38
Valid From	May 16 19:18:06 2013 GMT
Valid To	May 16 19:18:06 2021 GMT
SHA-1 Print	86:33:63:36:A3:17:2E:73:AB:67:90:DC:55:31:65:7A:67:58:91:D6

5.3.9.2 End Entity Information

ORC NFI PKI issues SHA-256 end entity certificates.

5.3.10 Raytheon

Raytheon is an Aero Defense partner through CertiPath. They currently have SHA-1 and SHA-256 infrastructures. They maintain infrastructure details at http://www.raytheon.com/pki/technical/index.html.

The Raytheon Root SHA-1 and SHA-256 Root CAs currently have a two-way cross-certificate relationship with the SHA-1 and SHA-256 CertiPath Bridge CAs respectively.

5.3.10.1 SHA-1 Trust Chain

TRUST ANCHOR	
Issuer	`OU=RaytheonRoot,O=CAs,DC=raytheon,DC=com`
Subject	`OU=RaytheonRoot,O=CAs,DC=raytheon,DC=com`
Serial #	`0X465D9A2A`
Valid From	`Jan 15 21:55:39 2014 GMT`
Valid To	`Jan 15 22:25:39 2024 GMT`
SHA-1 Print	`87:D3:E5:7C:C6:DF:B7:7C:7C:F0:D0:FC:D0:1D:6C:20:92:D0:47:62`

ISSUING CA	
Issuer	`OU=RaytheonRoot,O=CAs,DC=raytheon,DC=com`
Subject	`OU=class3,O=CAs,DC=raytheon,DC=com`
Serial #	`0x465D9BF7`
Valid From	`Apr  9 22:32:56 2014 GMT`
Valid To	`Feb 10 13:33:18 2022 GMT`
SHA-1 Print	`DA:5C:A3:26:66:F4:54:94:C9:1E:AC:D0:18:26:10:DA:CF:A4:FE:AB`

5.3.10.2 SHA-256 Trust Chain

TRUST ANCHOR	
Issuer	`CN=Raytheon Root CA,OU=RaytheonRoot-g2,O=CAs,DC=raytheon,DC=com`
Subject	`CN=Raytheon Root CA,OU=RaytheonRoot-g2,O=CAs,DC=raytheon,DC=com`
Serial #	`0x55132536`
Valid From	`Mar 25 20:45:18 2015 GMT`
Valid To	`Mar 25 21:15:18 2035 GMT`
SHA-1 Print	`FC:A0:EC:B4:01:32:21:7E:07:B1:65:25:62:D1:CB:24:DE:67:E7:1F`

ISSUING CA	
Issuer	`CN=Raytheon Root CA,OU=RaytheonRoot-g2,O=CAs,DC=raytheon,DC=com`
Subject	`CN=Raytheon Class 3 MASCA,OU=Class3-g2,O=cas,DC=raytheon,DC=com`
Serial #	`0x551326E7`
Valid From	`May 26 15:11:04 2015 GMT`
Valid To	`May 26 15:41:04 2023 GMT`
SHA-1 Print	`74:87:74:6F:25:33:30:75:18:8A:E9:B0:DF:93:A6:E1:73:B8:8A:33`

5.3.10.3 End Entity Information

Raytheon currently issues SHA-1 and SHA-256 end entity certificates only.

5.3.11 Symantec NFI PKI (formerly VeriSign NFI PKI)

Symantec Non-Federal Issuer (NFI) PKI provides PKI credentials to state and local Government as well as contractors. Symantec NFI issues two types of DoD approved certificates: PIV-Interoperable (PIV-I) certificates and Medium Hardware certificates. Symantec NFI has two SHA-256 trust chains as shown below. In addition to installing the proper trust chain, DoD relying parties that interoperate with Symantec NFI certificates must ensure that their applications support SHA-256. Symantec NFI PKI also has device Issuing CA certificates which are currently not included because they don’t meet the medium hardware assurance level requirement. Symantec NFI PKI has a two-way cross-certificate relationship between the VeriSign and Symantec Class 3 SSP Intermediate CAs and the Federal Bridge CA.

5.3.11.1 SHA-256 Trust Chain 1– Current

TRUST ANCHOR	
Issuer	CN=VeriSign Universal Root Certification Authority,OU=(c) 2008 VeriSign, Inc. - For authorized use only,OU=VeriSign Trust Network,O=VeriSign, Inc.,C=US
Subject	CN=VeriSign Universal Root Certification Authority,OU=(c) 2008 VeriSign, Inc. - For authorized use only,OU=VeriSign Trust Network,O=VeriSign, Inc.,C=US
Serial #	0x401AC46421B31321030EBBE4121AC51D
Valid From	Apr 2 00:00:00 2008 GMT
Valid To	Dec 1 23:59:59 2037 GMT
SHA-1 Print	36:79:CA:35:66:87:72:30:4D:30:A5:FB:87:3B:0F:A7:7B:B7:0D:54

INTERMEDIATE CA	
Issuer	CN=VeriSign Universal Root Certification Authority,OU=(c) 2008 VeriSign, Inc. - For authorized use only,OU=VeriSign Trust Network,O=VeriSign, Inc.,C=US
Subject	CN=VeriSign Class 3 SSP Intermediate CA - G2,OU=VeriSign Trust Network,O=VeriSign, Inc.,C=US
Serial #	0x316CEB691DCB2E153D9BFA8A121BD52D
Valid From	Dec 6 00:00:00 2010 GMT
Valid To	Dec 5 23:59:59 2020 GMT
SHA-1 Print	D1:D6:05:84:7B:A3:11:1C:83:EA:EF:32:E4:C8:E2:AE:93:61:50:54

BOOZ ALLEN HAMILTON ISSUING CA (USER CERTIFICATES ONLY)	
Issuer	CN=VeriSign Class 3 SSP Intermediate CA - G2,OU=VeriSign Trust Network,O=VeriSign, Inc.,C=US
Subject	CN=Booz Allen Hamilton CA 02,OU=Certification Authorities,O=Booz Allen Hamilton,C=US
Serial #	0x7B15016346C0BD9532EA3B3EE366E865
Valid From	Jul 31 00:00:00 2012 GMT
Valid To	Jul 30 23:59:59 2019 GMT
SHA-1 Print	F8:9A:25:F0:D3:5D:67:F9:45:40:CF:69:6E:79:86:06:88:98:59:C0

COMPUTER SCIENCES CORPORATION ISSUING CA (USER CERTIFICATES ONLY)	
Issuer	CN=VeriSign Class 3 SSP Intermediate CA - G2,OU=VeriSign Trust Network,O=VeriSign, Inc.,C=US
Subject	CN=CSC CA - 2,OU=NPS,O=Computer Sciences Corporation,C=US
Serial #	0x547B28C1E722F86897CF9ADF96940EC6
Valid From	Jun 20 00:00:00 2012 GMT
Valid To	Jun 19 23:59:59 2019 GMT
SHA-1 Print	B3:4B:9D:DF:3C:59:05:D1:28:D9:51:D5:0E:F9:7D:41:29:55:4B:BA

EID PASSPORT - RAPIDGATE PIV-I ISSUING CA (USER CERTIFICATES ONLY)	
Issuer	CN=VeriSign Class 3 SSP Intermediate CA - G2,OU=VeriSign Trust Network,O=VeriSign\, Inc.,C=US
Subject	CN=RAPIDGate PIV-I Agency CA,O=Eid Passport\, Inc.,C=US
Serial #	0x7C5123D5F59B9A2C88ED864873B1EE68
Valid From	May 17 00:00:00 2012 GMT
Valid To	May 16 23:59:59 2019 GMT
SHA-1 Print	DE:6E:C5:29:7A:56:FA:57:D0:16:62:5A:C3:CC:8A:F5:23:4B:39:6B

EID PASSPORT - RAPIDGATE PREMIER ISSUING CA (USER CERTIFICATES ONLY)	
Issuer	CN=VeriSign Class 3 SSP Intermediate CA - G2,OU=VeriSign Trust Network,O=VeriSign\, Inc.,C=US
Subject	CN=RAPIDGate Premier CA,O=Eid Passport\, Inc.,C=US
Serial #	0x1414A035C1288EC17AD8FD3D1171E211
Valid From	Dec 17 00:00:00 2013 GMT
Valid To	Dec 4 23:59:59 2020 GMT
SHA-1 Print	61:71:C2:76:18:99:6F:E4:E7:C2:48:F2:3F:17:51:59:8B:5E:0F:08

ICF INTERNATIONAL ISSUING CA (USER CERTIFICATES ONLY)	
Issuer	CN=VeriSign Class 3 SSP Intermediate CA - G2,OU=VeriSign Trust Network,O=VeriSign, Inc.,C=US
Subject	CN=ICFI PIV Interoperable CA,OU=ICF International,O=ICF Incorporated LLC,C=US
Serial #	0x7EF7F0186038DCFF4842A2D8F3570BA3
Valid From	Jan 18 00:00:00 2011 GMT
Valid To	Jan 17 23:59:59 2018 GMT
SHA-1 Print	14:77:93:46:E3:6F:D7:6D:66:84:B0:E7:46:D7:60:19:A9:41:EB:B6

MILLENIUM CHALLENGE CORPORATION ISSUING CA (USER CERTIFICATES ONLY)	
Issuer	CN=VeriSign Class 3 SSP Intermediate CA - G2,OU=VeriSign Trust Network,O=VeriSign, Inc.,C=US
Subject	CN=Millennium Challenge Corporation Medium HW CA – G2,OU=MCC,O=U.S. Government,C=US
Serial #	0x4CF5B1F83DE78A00C4FBAD4D5E761D08
Valid From	Feb 3 00:00:00 2011 GMT
Valid To	Feb 2 23:59:59 2018 GMT
SHA-1 Print	B7:81:96:70:B3:88:76:20:27:93:3B:A5:7D:FE:3A:88:52:6F:45:5F

U.S. SENATE ISSUING CA (USER CERTIFICATES ONLY)	
Issuer	CN=VeriSign Class 3 SSP Intermediate CA - G2,OU=VeriSign Trust Network,O=VeriSign, Inc.,C=US
Subject	CN=Senate PIV-I CA G2,OU=Office of the Sergeant at Arms,OU=U.S. Senate,O=U.S. Government,C=US
Serial #	0x0954E4BCD441044BCB144691027E0DB4
Valid From	Jul 21 00:00:00 2011 GMT
Valid To	Jul 20 23:59:59 2018 GMT
SHA-1 Print	4B:EA:1A:78:ED:4B:9B:E5:A4:12:34:EA:E8:D6:44:5D:9C:AB:74:72

5.3.11.2 SHA-256 Trust Chain 2 – Current

TRUST ANCHOR	
Issuer	CN=VeriSign Universal Root Certification Authority,OU=(c) 2008 VeriSign, Inc. - For authorized use only,OU=VeriSign Trust Network,O=VeriSign, Inc.,C=US
Subject	CN=VeriSign Universal Root Certification Authority,OU=(c) 2008 VeriSign, Inc. - For authorized use only,OU=VeriSign Trust Network,O=VeriSign, Inc.,C=US
Serial #	0x401AC46421B31321030EBBE4121AC51D
Valid From	Apr 2 00:00:00 2008 GMT
Valid To	Dec 1 23:59:59 2037 GMT
SHA-1 Print	36:79:CA:35:66:87:72:30:4D:30:A5:FB:87:3B:0F:A7:7B:B7:0D:54

INTERMEDIATE CA	
Issuer	CN=VeriSign Universal Root Certification Authority,OU=(c) 2008 VeriSign\, Inc. - For authorized use only,OU=VeriSign Trust Network,O=VeriSign\, Inc.,C=US
Subject	CN=Symantec Class 3 SSP Intermediate CA - G3,OU=Symantec Trust Network,O=Symantec Corporation,C=US
Serial #	0x45B1BEB5F3D47BFBC145F4D9179E22F2
Valid From	Sep 30 00:00:00 2014 GMT
Valid To	Sep 29 23:59:59 2024 GMT
SHA-1 Print	55:DB:7B:0B:02:A0:CD:64:4E:2B:B7:62:45:F8:F0:89:3A:E9:F9:A9

EID PASSPORT – LRA 2 ISSUING CA (USER CERTIFICATES ONLY)	
Issuer	CN=Symantec Class 3 SSP Intermediate CA - G3,OU=Symantec Trust Network,O=Symantec Corporation,C=US
Subject	CN=Eid Passport LRA 2 CA,OU=Eid Passport PIV-I LRA Network,O=Eid Passport\, Inc.,C=US
Serial #	0x74FA80B580B11F82CDE84EF3AD8E36A4
Valid From	Mar 10 00:00:00 2015 GMT
Valid To	Sep 28 23:59:59 2024 GMT
SHA-1 Print	03:35:E3:67:01:06:DA:48:DB:61:E0:06:65:FA:16:F8:D8:C1:10:AE

CSRA ISSUING CA (USER CERTIFICATES ONLY)	
Issuer	CN=Symantec Class 3 SSP Intermediate CA - G3,OU=Symantec Trust Network,O=Symantec Corporation,C=US
Subject	CN=CSRA FBCA C3 CA,OU=CSRA FBCA MedHW,O=CSC Government Solutions LLC,C=US
Serial #	0x48B53C25944E6ED645339ECF1079FD37
Valid From	Dec 17 00:00:00 2015 GMT
Valid To	Sep 28 23:59:59 2024 GMT
SHA-1 Print	FA:ED:5B:3A:A8:5B:FE:A0:BA:8B:A8:84:68:97:06:04:4D:FC:0E:C9

5.3.11.3 End Entity Information

Symantec NFI PKI issues SHA-256 end entity certificates.

5.3.12 Verizon Business NFI PKI

Verizon Business Non-Federal Issuer (NFI) PKI provides PKI credentials to state and local government as well as contractors. Verizon Business NFI PKI has one SHA-256 Trust Chain as shown below and has a two-way trust relationship with the Federal Bridge CA. DoD relying parties that wish to interoperate with Verizon Business NFI PKI should ensure their applications support SHA-256.

	TRUST ANCHOR
Issuer	CN=CT-CSSP-CA-A1,OU=PKI,OU=Services,O=Cybertrust,C=US
Subject	CN=CT-CSSP-CA-A1,OU=PKI,OU=Services,O=Cybertrust,C=US
Serial #	0x01
Valid From	Aug 6 20:27:13 2008 GMT
Valid To	Aug 6 20:23:03 2028 GMT
SHA-1 Print	98:C2:ED:E6:51:89:EE:1B:BF:CB:5B:13:B5:4E:72:82:15:36:E1:9D

	ISSUING CA
Issuer	CN=CT-CSSP-CA-A1,OU=PKI,OU=Services,O=Cybertrust,C=US
Subject	CN=CT-GEN-MSO-CA-B1,OU=PKI,OU=Services,O=Cybertrust,C=US
Serial #	0x67
Valid From	Dec 5 18:45:46 2008 GMT
Valid To	Dec 5 18:45:46 2018 GMT
SHA-1 Print	73:00:AD:0B:CB:71:F2:E2:FE:C3:B9:A3:15:1B:27:87:2D:54:64:97

5.3.12.1 End Entity Information

Verizon Business NFI PKI issues SHA-256 end entity certificates.

5.4 Foreign, Allied, or Coalition Partner PKIs or other PKIs (Category III PKIs)

Foreign, Allied, or Coalition Partners are classified in the DoD External Interoperability Plan as Category III PKIs. In addition to meeting the technical requirements and successfully completing JITC testing, Category III PKIs must sign a Cross Certification Arrangement (CCA). The Category III PKI Certificate Policy will be mapped to the DoD PKI Certificate Policy in accordance with DoD PKI policy. With respect to CCEB, the CCA will comply with Allied Communications Publication (ACP) 185 which is the framework for PKI Interoperability between CCEB partner nations. Category III partners can be approved at Medium Hardware or Device and often have additional assurance levels. For applications that cannot perform cross-certificate path validation, direct trust may be used with additional consideration. DoD users and systems that choose to directly trust a Category III PKI should install the appropriate trust chain into the application or system trust store and ensure that the application is inspecting the certificate to ensure it asserts a DoD approved certificate policy OID. For more information DoD approved OIDs, refer to Section 6, Assurance Levels.

5.4.1 Australian Defence Organisation (ADO) PKI

The Australian Defence Organisation (ADO) PKI provides PKI credentials to military and civilian personnel. Subscribers include any individual that has been approved as having a requirement to be authenticated as affiliated with ADO. Subscribers include:

- Defence personnel (permanent and reserve members of the Australian Defence Force (ADF), and Australian Public Service (APS) employees)
- Members of the ADF Cadets
- Contractors, Consultants and Professional Service Providers (individuals)

- Other individuals approved by ADO as having a requirement for an ADO Certificate.
- Secure Communications Resource Certificates are only issued to non-person entities (NPE), not individuals

ADO PKI has two SHA-1 Trust Chains as shown below and has a two-way trust relationship with US DoD CCEB IRCA1. DoD relying parties that wish to interoperate with ADO cross-certificates should ensure their applications support cross certificate path processing.

5.4.1.1 *SHA-1 Cross-Certificate Trust Chain – US to Australia - Current*

TRUST ANCHOR	
Issuer	CN=US DoD CCEB Interoperability Root CA 1,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=US DoD CCEB Interoperability Root CA 1,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x01
Valid From	Nov 29 17:47:23 2010 GMT
Valid To	Nov 24 17:47:23 2030 GMT
SHA-1 Print	E0:41:0B:4A:58:2F:B1:C4:DD:52:B0:31:2B:A3:F4:39:4D:4F:01:B8

US DOD CCEB INTEROPERABILITY ROOT CA 1-ADOCA03 CROSS CERTIFICATE	
Issuer	CN=US DoD CCEB Interoperability Root CA 1,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=ADOCA03,OU=CAs,OU=PKI,OU=DoD,O=GOV,C=AU
Serial #	0x012C
Valid From	Apr 16 12:51:41 2014 GMT
Valid To	Apr 16 12:51:41 2017 GMT
SHA-1 Print	A6:5C:12:55:BE:19:EB:58:2B:4A:00:A7:F0:E5:BB:84:58:7D:A8:96

ADOCA03-ADOCA016 CROSS CERTIFICATE	
Issuer	CN=ADOCA03,OU=CAs,OU=PKI,OU=DoD,O=GOV,C=AU
Subject	CN=ADOCA016,OU=CAs,OU=PKI,OU=DoD,O=GOV,C=AU
Serial #	0x65C85DF22A3E9234346EBA21C8B718770630AAD1
Valid From	Dec 17 23:48:09 2013 GMT
Valid To	Dec 17 23:48:09 2016 GMT
SHA-1 Print	A7:8D:76:29:A7:8C:35:7B:DE:7A:D6:AF:84:D7:C6:18:04:33:4D:7C

5.4.1.2 *SHA-1 Direct Trust Chain – Current*

ACP 185 specifies that cross-certificate trust should be used for PKI validation between partner nations. Direct trust should only be used in special cases where cross-certificates cannot be processed by the relying party application. Using Direct Trust may cause relying party systems to inadvertently inherit trust from unapproved PKIs that are cross certified with ADO. Any direct trust implementations must also use the Trust Anchor Constraints Tool (TACT) or implement another OID and name constraint filtering mechanism to prevent acceptance of certificates from unapproved PKIs and/or assurance levels.

TRUST ANCHOR	
Issuer	CN=ADOCA02,OU=CAs,OU=PKI,OU=DoD,O=GOV,C=AU
Subject	CN=ADOCA02,OU=CAs,OU=PKI,OU=DoD,O=GOV,C=AU
Serial #	0x0715
Valid From	Sep 1 04:26:07 2011 GMT
Valid To	Jan 27 02:31:24 2019 GMT
SHA-1 Print	84:42:9D:9F:E2:E7:3A:0D:C8:AA:0A:E0:A9:02:F2:74:99:33:FE:02

	ISSUING CA
Issuer	CN=ADOCA02,OU=CAs,OU=PKI,OU=DoD,O=GOV,C=AU
Subject	CN=ADOCA016,OU=CAs,OU=PKI,OU=DoD,O=GOV,C=AU
Serial #	0x396001BD02A6000145FCFD991537A2F9C7D2A252
Valid From	Dec 17 23:36:16 2013 GMT
Valid To	Dec 17 23:36:16 2018 GMT
SHA-1 Print	SHA1 Fingerprint=E8:C2:59:43:6E:B9:9B:91:40:F9:E5:1D:71:7A:20:B5:27:8C:C6:C5

5.4.1.3 End Entity Information

ADO PKI currently issues SHA-1 end entity certificates only.

6.0 Assurance Levels[17]

Assurance levels are represented by Certificate Policy Object Identifiers (OIDs) which are asserted in the *Certificate Policies* x509 certificate extension.[18] Every PKI has its own certificate policy OIDs which are registered uniquely to the organization and are defined in the PKI's certificate policy. Since each PKI has different certificate policy OIDs which are separately defined, it is easier to speak in terms of relative Federal PKI (FPKI) assurance levels. This especially works well since part of the cross certification process includes mapping equivalent policies. In the cross certification trust model, a PKI can enforce a set of acceptable certificate policies through policy mappings. *Policy Mappings* is an x509 certificate extension used in cross-certificates. In DoD, policy mappings are defined in the cross-certificate issued by the Interoperability Root CAs. DoD PKI only maps to FBCA medium hardware assurance level or higher, which causes all lower assurance levels to be invalid according to the standard. In the direct trust model, the responsibility is on the data owner to enforce the DoD allowable set of policies. This can be done through defining an initial-policy-set for applications that support it or through some other means of certificate policy OID restriction or filtering. Some commercial applications such as the Trust Anchor Constraints Tool (TACT), Webcullis or Threat Management Gateway support this functionality.[19]

DoD PKI and ECA PKI, software certificates are allowed as an approved form of identity credential per DoD instruction 8520.03. However, DoD Instruction 8520.02, Enclosure 3 Paragraph 1c states: "While DoD medium assurance (software) certificates are acceptable for use within the DoD, they are primarily intended for use in servers and other non-person entities (e.g., SSL certificates), and their use for identifying people (i.e., issuance of an identity certificate for a person) should be minimized".

[17] For more information on assurance levels, see NIST 800-63, Electronic Authentication Guideline http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

[18] RFC 5280 can be found at http://www.ietf.org/rfc/rfc5280.txt

[19] Webcullis can be found at http://pkif.sourceforge.net/webcullis.html and Threat Management Gateway can be found at http://www.microsoft.com/forefront/threat-management-gateway/en/us/default.aspx

6.1 DoD Assurance Levels

All DoD assurance levels are permitted for use within DoD. Although some DoD relying parties may wish to further restrict the set of acceptable DoD policies. For instance, some application owners may require hardware certificates and not accept software certificates which have a lower assurance level. The DoD certificate policy OIDs are shown below. More information is provided in the DoD Certificate Policy.[20]

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	ALLOWABLE PER POLICY (Y/N)
2.16.840.1.101.2.1.11.2	id-US-dod-basic[21]	Yes. All DoD Certificate Policies are allowed per DoD policy.
2.16.840.1.101.2.1.11.4	id-US-dod-FORTEZZA[22]	
2.16.840.1.101.2.1.11.5	id-US-dod-medium	
2.16.840.1.101.2.1.11.6	id-US-dod-type1	
2.16.840.1.101.2.1.11.9	id-US-dod-mediumhardware	
2.16.840.1.101.2.1.11.10	id-US-dod-PIV-Auth[23]	
2.16.840.1.101.2.1.11.17	id-US-dod-mediumNPE	
2.16.840.1.101.2.1.11.18	id-US-dod-medium-2048	
2.16.840.1.101.2.1.11.19	id-US-dod-mediumHardware-2048	
2.16.840.1.101.2.1.11.20	id-US-dod-PIV-Auth-2048[24]	
2.16.840.1.101.2.1.11.31	id-US-dod-peerInterop[25]	
2.16.840.1.101.2.1.11.36	id-US-dod-mediumNPE-112	
2.16.840.1.101.2.1.11.37	id-US-dod-mediumNPE-128	
2.16.840.1.101.2.1.11.39	id-US-dod-medium-112	
2.16.840.1.101.2.1.11.40	id-US-dod-medium-128	
2.16.840.1.101.2.1.11.42	id-US-dod-mediumHardware-112	
2.16.840.1.101.2.1.11.43	id-US-dod-mediumHardware-128	

6.2 ECA PKI Assurance Levels

All ECA PKI assurance levels are permitted for use within DoD. Although some relying parties may wish to further restrict the set of acceptable ECA policies. For instance, some application owners may require hardware certificates and not accept software certificates which have a lower assurance level. The ECA certificate policy OIDs are shown below. More information is provided in the ECA Certificate Policy.[26]

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	ALLOWABLE PER POLICY (Y/N)
2.16.840.1.101.3.2.1.12.1	id-eca-medium	Yes. All ECA Certificate Policies are allowed per DoD policy
2.16.840.1.101.3.2.1.12.2	id-eca-medium-hardware	
2.16.840.1.101.3.2.1.12.3	id-eca-medium-token	
2.16.840.1.101.3.2.1.12.4	id-eca-medium-sha256	
2.16.840.1.101.3.2.1.12.5	id-eca-medium-token-sha256	
2.16.840.1.101.3.2.1.12.6	id-eca-medium-hardware-pivi	
2.16.840.1.101.3.2.1.12.7	id-eca-cardauth-pivi	
2.16.840.1.101.3.2.1.12.8	id-eca-contentsigning-pivi[27]	
2.16.840.1.101.3.2.1.12.9	id-eca-medium-device-sha256	
2.16.840.1.101.3.2.1.12.10	id-eca-medium-hardware-sha256	

[20] The DoD Certificate Policy can be found at http://iase.disa.mil/pki-pke/Documents/unclass-dod_cp_v10-5.pdf

[21] id-US-dod-basic is not used operationally within DoD

[22] id-US-dod-high is not used operationally within DoD.

[23] id-US-dod-PIV-Auth is not used operationally within DoD.

[24] id-US-dod-PIV-Auth-2048 is not used operationally within DoD.

[25] The Peer Interop OID is only used for cross-certificates issued to external PKIs that cannot demonstrate comparability to one or more requirements of Medium Assurance and the DoD determines that there is a need for interoperation and acceptance of certificates issued by the external PKIs. Relying Parties need to ensure that it is appropriate to use the certificate issued by a PKI that maps to Peer Interop before enabling systems to accept these certificates.

[26] The ECA Certificate Policy can be found at http://iase.disa.mil/pki-pke/Documents/unclass-dod_eca_v4-3_4jan12.pdf

[27] All contentsigning OIDs are intended only for use in digitally signing data objects on a PIV-I smart card and shall not be used for any other purpose. Content Signing PIV-I certificates shall only be issued to Card Management Systems.

6.3 Federal PKI (FPKI) Assurance Levels

All DoD approved external PKIs are cross certified with FPKI, either directly or through an SSP or another bridge. Part of the cross certification process includes mapping organizational certificate policy OIDs to equivalent FPKI policy OIDs. DoD currently has cross-certificate relationships with two Federal PKI CAs. DoD Interoperability Root CA 1 is two-way cross certified with the SHA-1 Federal Root CA in order to support cross-certificate trust with our SHA-1 partners and DoD Interoperability Root CA 2 is two-way cross certified with the Federal Bridge CA to support cross-certificate trust with our SHA-256 partners. DoD enforces RFC 5280 constraints in its cross-certificates and only maps to FPKI policies which are at id-fpki-SHA1-hardware level or higher, causing all lower assurance certificate policies to be considered invalid by policy. Application owners that interoperate using direct trust will be responsible for ensuring that only certificates at DoD allowed assurance levels are accepted by their applications. In order to comply with NIST cryptographic guidance, FPKI recently introduced a significant architectural redesign[28]. The redesign introduced two new SHA-256 FPKI systems: Federal Bridge CA and Federal Common Policy CA. Additionally they deployed the SHA-1 Federal Root CA to support FPKI partners that remain SHA-1. FPKI has decommissioned the legacy FBCA (ou=Entrust) and Common Policy systems.

6.3.1 SHA-1 Federal PKI Assurance

FPKI partners that are cross certified with the SHA-1 Federal Root CA must assert and map to specific SHA-1 distinguishing policies shown below.

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	ALLOWABLE PER POLICY (Y/N)
2.16.840.1.101.3.2.1.3.21	id-fpki-SHA1-medium-CBP	No
2.16.840.1.101.3.2.1.3.22	id-fpki-SHA1-mediumHW-CBP	No
2.16.840.1.101.3.2.1.3.23	id-fpki-SHA1-policy	No
2.16.840.1.101.3.2.1.3.24	id-fpki-SHA1-hardware	Yes
2.16.840.1.101.3.2.1.3.25	id-fpki-SHA1-devices	No

6.3.2 Federal PKI Assurance Levels

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	ALLOWABLE PER POLICY (Y/N)
2.16.840.1.101.3.2.1.3.1	id-fpki-certpcy-rudimentaryAssurance	No
2.16.840.1.101.3.2.1.3.2	id-fpki-certpcy-basicAssurance	No
2.16.840.1.101.3.2.1.3.3	id-fpki-certpcy-mediumAssurance	No
2.16.840.1.101.3.2.1.3.4	id-fpki-certpcy-highAssurance	Yes
2.16.840.1.101.3.2.1.3.5	fpki-certpcy-testAssurance	No
2.16.840.1.101.3.2.1.3.6	id-fpki-common-policy	No
2.16.840.1.101.3.2.1.3.7	id-fpki-common-hardware	Yes
2.16.840.1.101.3.2.1.3.8	id-fpki-common-devices	No
2.16.840.1.101.3.2.1.3.9	id-eGov-Level1	No
2.16.840.1.101.3.2.1.3.10	id-eGov-Level2	No
2.16.840.1.101.3.2.1.3.11	id-eGov-Applications	No
2.16.840.1.101.3.2.1.3.12	id-fpki-certpcy-mediumHardware	Yes
2.16.840.1.101.3.2.1.3.13	id-fpki-common-authentication	Yes
2.16.840.1.101.3.2.1.3.14	id-fpki-certpcy-medium-CBP	No
2.16.840.1.101.3.2.1.3.15	id-fpki-certpcy-mediumHW-CBP	No
2.16.840.1.101.3.2.1.3.16	id-fpki-common-High	Yes
2.16.840.1.101.3.2.1.3.17	id-fpki-common-cardAuth	Yes-Physical access only

[28] NIST Special Publication 800-78-3 can be found at http://csrc.nist.gov/publications/nistpubs/800-78-3/sp800-78-3.pdf

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	ALLOWABLE PER POLICY (Y/N)
2.16.840.1.101.3.2.1.3.18	id-fpki-certpcy-pivi-hardware	Yes
2.16.840.1.101.3.2.1.3.19	id-fpki-certpcy-pivi-cardAuth	Yes-Physical access only
2.16.840.1.101.3.2.1.3.20	id-fpki-certpcy-pivi-contentSigning	Yes
2.16.840.1.101.3.2.1.3.28	id-eGov-Level1-IdP	No
2.16.840.1.101.3.2.1.3.29	id-eGov-Level2-IdP	No
2.16.840.1.101.3.2.1.3.30	id-eGov-Level3-IdP	No
2.16.840.1.101.3.2.1.3.31	id-eGov-Level4-IdP	No
2.16.840.1.101.3.2.1.3.32	id-eGov-BAE-Broker	No
2.16.840.1.101.3.2.1.3.33	id-eGov-RelyingParty	No
2.16.840.1.101.3.2.1.3.34	id-eGov-MetaSigner	No
2.16.840.1.101.3.2.1.3.35	id-eGov-MetaSigner-Hardware	No
2.16.840.1.101.3.2.1.3.36	id-fpki-common-devicesHardware	Yes
2.16.840.1.101.3.2.1.3.37	id-fpki-certpcy-mediumDevice	No. Currently under consideration.
2.16.840.1.101.3.2.1.3.38	id-fpki-certpcy-mediumDeviceHardware	Yes
2.16.840.1.101.3.2.1.3.39	id-fpki-common-piv-contentSigning	Yes
2.16.840.1.101.3.2.1.3.40	id-fpki-common-pivAuth-derived	No
2.16.840.1.101.3.2.1.3.41	id-fpki-common-pivAuth-derived-hardware	No

6.4 Entrust SSP PKI Assurance Levels

Entrust SSP PKI currently has a one-way cross-certificate relationship with Federal Common Policy CA. The Federal Common Policy CA issued a certificate to Entrust Managed Services Root CA, but there is no reverse certificate. Entrust SSP PKI currently asserts the following certificate policies in its certificates, five of which are permitted by DoD policy:

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
2.16.840.1.101.3.2.1.3.6	id-fpki-common-policy	Yes-asserted	No
2.16.840.1.101.3.2.1.3.7	id-fpki-common-hardware	Yes-asserted	Yes
2.16.840.1.101.3.2.1.3.8	id-fpki-common-devices	Yes-asserted	No
2.16.840.1.101.3.2.1.3.13	id-fpki-common-authentication	Yes-asserted	Yes
2.16.840.1.101.3.2.1.3.17	id-fpki-common-cardAuth	Yes-asserted	Yes-Physical access only
2.16.840.1.101.3.2.1.3.36	id-fpki-common-devicesHardware	Yes-asserted	Yes
2.16.840.1.101.3.2.1.3.39	id-fpki-common-piv-contentSigning	Yes-asserted	Yes
2.16.840.1.101.3.2.1.3.40	id-fpki-common-pivAuth-derived	Yes-asserted	No
2.16.840.1.101.3.2.1.3.41	id-fpki-common-pivAuth-derived-hardware	Yes-asserted	No

6.5 ORC SSP PKI Assurance Levels

ORC SSP PKI has a one-way cross-certificate relationship with FPKI, with a certificate issued from Federal Common Policy CA to ORC SSP 3.

6.5.1 ORC SSP PKI Asserted Policies

ORC SSP PKI currently asserts the following certificate policies in its certificates, three of which are permitted by DoD policy:

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
2.16.840.1.101.3.2.1.3.6	id-fpki-common-policy	Yes-asserted	No
2.16.840.1.101.3.2.1.3.7	id-fpki-common-hardware	Yes-asserted	Yes
2.16.840.1.101.3.2.1.3.8	id-fpki-common-devices	Yes-asserted	No

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
2.16.840.1.101.3.2.1.3.13	id-fpki-common-authentication	Yes-asserted	Yes
2.16.840.1.101.3.2.1.3.17	id-fpki-common-cardAuth	Yes-asserted	Yes-Physical access only
2.16.840.1.101.3.2.1.3.36	id-fpki-common-devicesHardware	Yes-asserted	Yes
2.16.840.1.101.3.2.1.3.39	id-fpki-common-piv-contentSigning	Yes-asserted	Yes

6.6 Department of State PKI Assurance Levels

Department of State currently has a two-way cross-certificate relationship with Federal Common Policy CA. It currently asserts the following certificate policies in its certificates, six of which are permitted by DoD policy:

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
2.16.840.1.101.3.2.1.6.1	state-basic	Yes. Mapped	No
2.16.840.1.101.3.2.1.6.2	state-low	Yes. Mapped	No
2.16.840.1.101.3.2.1.6.3	state-moderate	Yes. Mapped	No
2.16.840.1.101.3.2.1.6.4	state-high	Yes. Mapped	Yes
2.16.840.1.101.3.2.1.6.12	state-medHW	Yes. Mapped	Yes
2.16.840.1.101.3.2.1.6.37	state-certpcy-mediumDevice	No	No
2.16.840.1.101.3.2.1.6.38	state-certpcy-mediumDeviceHardware	No	No
2.16.840.1.101.3.2.1.3.6	id-fpki-common-policy	Yes. Asserted	No
2.16.840.1.101.3.2.1.3.7	id-fpki-common-hardware	Yes. Asserted	Yes
2.16.840.1.101.3.2.1.3.8	id-fpki-common-devices	Yes. Asserted	No
2.16.840.1.101.3.2.1.3.13	id-fpki-common-authentication	Yes. Asserted	Yes
2.16.840.1.101.3.2.1.3.16	id-fpki-common-high	Yes. Asserted	Yes
2.16.840.1.101.3.2.1.3.17	id-fpki-common-cardAuth	Yes. Asserted	Yes-Physical access only

6.7 U.S. Treasury SSP PKI Assurance Levels

U.S Treasury Root CA currently has a two-way cross-certificate relationship with Federal Common Policy CA. U.S. Treasury SSP PKI currently asserts the following certificate policies in its certificates, six of which are permitted by DoD policy:

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
2.16.840.1.101.3.2.1.5.2	id-treasury-certpcy-rudimentary	Yes. Mapped	No
2.16.840.1.101.3.2.1.5.3	id-treasury-certpcy-basicindividual	Yes. Mapped	No
2.16.840.1.101.3.2.1.5.4	id-treasury-certpcy-mediumhardware	Yes. Mapped	Yes
2.16.840.1.101.3.2.1.5.5	id-treasury-certpcy-high	Yes. Mapped	Yes
2.16.840.1.101.3.2.1.5.7	id-treasury-certpcy-medium	Yes. Mapped	No
2.16.840.1.101.3.2.1.5.8	id-treasury-certpcy-basicorganizational	No.	No
2.16.840.1.101.3.2.1.3.1	id-fpki-certpcy-rudimentaryAssurance	Yes. Asserted	No
2.16.840.1.101.3.2.1.3.2	id-fpki-certpcy-basicAssurance	Yes. Asserted	No
2.16.840.1.101.3.2.1.3.6	id-fpki-common-policy	Yes. Asserted	No
2.16.840.1.101.3.2.1.3.7	id-fpki-common-hardware	Yes. Asserted	Yes
2.16.840.1.101.3.2.1.3.8	id-fpki-common-devices	Yes. Asserted	No

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
2.16.840.1.101.3.2.1.3.13	id-fpki-common-authentication	Yes. Asserted	Yes
2.16.840.1.101.3.2.1.3.16	id-fpki-common-high	Yes. Asserted	Yes
2.16.840.1.101.3.2.1.3.17	id-fpki-common-cardAuth	Yes. Asserted	Yes-Physical access only
2.16.840.1.101.3.2.1.3.36	id-fpki-common-devicesHardware	Yes. Asserted	Yes
2.16.840.1.101.3.2.1.3.39	id-fpki-common-piv-contentSigning	Yes. Asserted	Yes
2.16.840.1.101.3.2.1.3.40	id-fpki-common-pivAuth-derived	Yes. Asserted	No
2.16.840.1.101.3.2.1.3.41	id-fpki-common-pivAuth-derived-hardware	Yes. Asserted	No
2.16.840.1.101.3.2.1.15.8	id-dhs-certpcy-internalNpe	No	No

6.8 *Symantec SSP PKI Assurance Levels*

Symantec SSP SHA-2 PKI is subordinate to Federal Common Policy CA which has a two-way cross-certificate with FBCA and several legacy PKIs. Federal Common Policy is also the trust anchor for the other SSPs.

6.8.1 Symantec SSP PKI Asserted Policies

Symantec SSP PKI currently asserts the following certificate policies in its certificates, four of which are permitted by DoD policy:

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
2.16.840.1.101.3.2.1.3.6	id-fpki-common-policy	Yes. Asserted	No
2.16.840.1.101.3.2.1.3.7	id-fpki-common-hardware	Yes. Asserted	Yes
2.16.840.1.101.3.2.1.3.8	id-fpki-common-devices	Yes. Asserted	No
2.16.840.1.101.3.2.1.3.13	id-fpki-common-authentication	Yes. Asserted	Yes
2.16.840.1.101.3.2.1.3.16	id-fpki-common-High	Yes. Asserted	Yes
2.16.840.1.101.3.2.1.3.17	id-fpki-common-cardAuth	Yes. Asserted	Yes-Physical access only

6.8.2 Symantec SSP PKI Inherited Policies

Although Symantec SSP PKI only asserts the certificate policies in section 6.8.1, the parent of its SHA-256 PKI, Federal Common Policy CA, has issued subordinate CA certificates to each SSP as well as cross-certificates to Department of State and Federal Bridge CA. Federal Common Policy CA asserts the following certificate policies in its cross-certificate to FBCA, extending trust to the entire FBCA community at many assurance levels.

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
2.16.840.1.101.3.2.1.3.1	id-fpki-certpcy-rudimentaryAssurance	Yes. Asserted	No
2.16.840.1.101.3.2.1.3.2	id-fpki-certpcy-basicAssurance	Yes. Asserted	No
2.16.840.1.101.3.2.1.3.6	id-fpki-common-policy	Yes. Mapped	No
2.16.840.1.101.3.2.1.3.7	id-fpki-common-hardware	Yes. Mapped	Yes
2.16.840.1.101.3.2.1.3.8	id-fpki-common-devices	Yes. Asserted	No
2.16.840.1.101.3.2.1.3.13	id-fpki-common-authentication	Yes. Asserted	Yes
2.16.840.1.101.3.2.1.3.14	id-fpki-certpcy-medium-CBP	Yes. Asserted	No
2.16.840.1.101.3.2.1.3.15	id-fpki-certpcy-mediumHW-CBP	Yes. Asserted	No
2.16.840.1.101.3.2.1.3.16	id-fpki-common-High	Yes. Mapped	Yes

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
2.16.840.1.101.3.2.1.3.17	id-fpki-common-cardAuth	Yes. Asserted	Yes-Physical access only
2.16.840.1.101.3.2.1.3.18	id-fpki-certpcy-pivi-hardware	Yes. Asserted	Yes
2.16.840.1.101.3.2.1.3.19	id-fpki-certpcy-pivi-cardAuth	Yes. Asserted	Yes-Physical access only
2.16.840.1.101.3.2.1.3.20	id-fpki-certpcy-pivi-contentSigning	Yes. Asserted	Yes

6.9 *Verizon Business SSP PKI Assurance Levels*

Verizon Business SSP PKI is subordinate to Federal Common Policy CA which has a two-way cross-certificate with FBCA and several legacy PKIs. Federal Common Policy is also the trust anchor for the other SSPs.

6.9.1 Verizon Business SSP PKI Asserted Policies

Verizon Business SSP PKI currently asserts the following certificate policies in its certificates, three of which are permitted by DoD policy:

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
2.16.840.1.101.3.2.1.3.6	id-fpki-common-policy	Yes-asserted	No
2.16.840.1.101.3.2.1.3.7	id-fpki-common-hardware	Yes-asserted	Yes
2.16.840.1.101.3.2.1.3.8	id-fpki-common-devices	Yes-asserted	No
2.16.840.1.101.3.2.1.3.13	id-fpki-common-authentication	Yes-asserted	Yes
2.16.840.1.101.3.2.1.3.17	id-fpki-common-cardAuth	Yes-asserted	Yes-Physical access only

6.9.2 Verizon Business SSP PKI Inherited Policies

Although Verizon Business SSP PKI only asserts the certificate policies in section 6.9.1, its parent, Federal Common Policy CA, has issued subordinate CA certificates to each SSP as well as cross-certificates to Department of State and FBCA. Federal Common Policy CA asserts the following certificate policies in its cross-certificate to FBCA, extending trust to the entire FBCA community at many assurance levels.

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
2.16.840.1.101.3.2.1.3.1	id-fpki-certpcy-rudimentaryAssurance	Yes. Asserted	No
2.16.840.1.101.3.2.1.3.2	id-fpki-certpcy-basicAssurance	Yes. Asserted	No
2.16.840.1.101.3.2.1.3.6	id-fpki-common-policy	Yes. Mapped	No
2.16.840.1.101.3.2.1.3.7	id-fpki-common-hardware	Yes. Mapped	Yes
2.16.840.1.101.3.2.1.3.8	id-fpki-common-devices	Yes. Asserted	No
2.16.840.1.101.3.2.1.3.13	id-fpki-common-authentication	Yes. Asserted	Yes
2.16.840.1.101.3.2.1.3.14	id-fpki-certpcy-medium-CBP	Yes. Asserted	No
2.16.840.1.101.3.2.1.3.15	id-fpki-certpcy-mediumHW-CBP	Yes. Asserted	No
2.16.840.1.101.3.2.1.3.16	id-fpki-common-High	Yes. Mapped	Yes
2.16.840.1.101.3.2.1.3.17	id-fpki-common-cardAuth	Yes. Asserted	Yes-Physical access only
2.16.840.1.101.3.2.1.3.18	id-fpki-certpcy-pivi-hardware	Yes. Asserted	Yes
2.16.840.1.101.3.2.1.3.19	id-fpki-certpcy-pivi-cardAuth	Yes. Asserted	Yes-Physical access only
2.16.840.1.101.3.2.1.3.20	id-fpki-certpcy-pivi-contentSigning	Yes. Asserted	Yes

6.10 Boeing PKI Assurance Levels

Boeing currently has a two-way cross-certificate relationship with the SHA-1 CertiPath Bridge CA. The SHA-1 CertiPath Bridge CA has a two-way cross-certificate relationship with the SHA-1 Federal Root CA. Boeing currently asserts the following certificate policies in its certificates, one of which is permitted by DoD policy:

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
1.3.6.1.4.1.73.15.3.1.4	id-mediumSoftware-SHA-1	Yes	No
1.3.6.1.4.1.73.15.3.1.5	id-mediumHardware-SHA-1	Yes	Yes
1.3.6.1.4.1.73.15.3.1.8	id-mediumCBPSoftware-SHA-1	No	No
1.3.6.1.4.1.73.15.3.1.9	id-mediumCBPHardware-SHA-1	No	No
1.3.6.1.4.1.73.15.3.1.10	id-mediumHardware-cardAuthentication-SHA1	No	No
1.3.6.1.4.1.73.15.3.1.11	id-mediumSoftware-SHA256	Yes	No
1.3.6.1.4.1.73.15.3.1.12	id-mediumHardware-SHA256	Yes	Yes
1.3.6.1.4.1.73.15.3.1.13	id-mediumCBPSoftware-SHA256	No	No
1.3.6.1.4.1.73.15.3.1.14	id-mediumCBPHardware-SHA256	No	No
1.3.6.1.4.1.73.15.3.1.15	id-mediumHardware-cardAuthentication-SHA256	Yes	Yes – Physical Access Only
1.3.6.1.4.1.73.15.3.1.16	id-mediumHardware-contentSigning-SHA1	Yes	Yes
1.3.6.1.4.1.73.15.3.1.17	id-mediumHardware-contentSigning-SHA256	Yes	Yes

6.11 Carillon Federal Services PKI Assurance Levels

Carillon currently has a two-way cross-certificate relationship with the (SHA-256) CertiPath Bridge CA – G2. It currently asserts the following certificate policies in its certificates, four of which are permitted by DoD policy:

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
1.3.6.1.4.1.45606.3.1.1	id-CFSINFRASTRUCTURE	No	No
1.3.6.1.4.1.45606.3.1.2	id-CFSINFRASTRUCTURE-256	No	No
1.3.6.1.4.1.45606.3.1.3	id-basicSoftware	No	No
1.3.6.1.4.1.45606.3.1.4	id-basicHardware	No	No
1.3.6.1.4.1.45606.3.1.7	id-mediumSoftware	No	No
1.3.6.1.4.1.45606.3.1.8	id-mediumHardware	No	No
1.3.6.1.4.1.45606.3.1.9	id-basicSoftware-256	No	No
1.3.6.1.4.1.45606.3.1.10	id-basicHardware-256	No	No
1.3.6.1.4.1.45606.3.1.11	id-mediumSoftware-256	No	No
1.3.6.1.4.1.45606.3.1.12	id-mediumHardware-256	Yes	Yes
1.3.6.1.4.1.45606.3.1.20	id-AIVHardware	Yes	Yes
1.3.6.1.4.1.45606.3.1.21	id-AIVCardAuth	Yes	Yes – Physical Access Only
1.3.6.1.4.1.45606.3.1.22	id-AIVContentSigning	Yes	Yes

NOTE: AIV (Advanced Identity Verification) enables the issuance of smart cards that are technically interoperable with United States Federal Government Personal Identity Verification (PIV) Card readers and applications as well as PIV-Interoperable (PIV-I) card readers and applications. AIV fully maps to PIV-I specification as defined by the U.S. Federal Government.[29]

[29] Carillon Federal Services Inc. Public Key Infrastructure Certificate Policy, *CFS-POL-007,* https://pub.carillonfedserv.com/CertificatePolicy.pdf August 28th, 2015.

6.12 CertiPath Bridge Assurance Levels[30]

CertiPath an organization that provides bridge services and has two bridge CAs that are cross certified with Federal PKI. They have a SHA-1 CertiPath Bridge CA, which is cross certified with the SHA-1 Federal Root CA and a (SHA-256) CertiPath Bridge CA – G2 which is cross certified with Federal Bridge CA. CertiPath vets and cross-certifies commercial and Aero/Defense partners to include PIV-Interoperable (PIV-I) partners.

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
1.3.6.1.4.1.24019.1.1.1.1	id-mediumSoftware	Yes. Mapped	No
1.3.6.1.4.1.24019.1.1.1.2	id-mediumHardware	Yes. Mapped	Yes
1.3.6.1.4.1.24019.1.1.1.3	id-highHardware	Yes. Mapped	Yes
1.3.6.1.4.1.24019.1.1.1.4	id-mediumCBPSoftware	Yes. Mapped	No
1.3.6.1.4.1.24019.1.1.1.5	id-mediumCBPHardware	Yes. Mapped	No
1.3.6.1.4.1.24019.1.1.1.6	id-highCBPHardware	No.	No
1.3.6.1.4.1.24019.1.1.1.7	id-IceCAP-hardware	Yes. Mapped	Yes
1.3.6.1.4.1.24019.1.1.1.8	id-IceCAP-cardAuth	Yes. Mapped	Yes-Physical access only
1.3.6.1.4.1.24019.1.1.1.9	id-IceCAP-contentSigning	Yes. Mapped	Yes
1.3.6.1.4.1.24019.1.1.1.17	id-variant-mediumSoftware	Yes. Mapped	No
1.3.6.1.4.1.24019.1.1.1.18	id-variant-mediumHardware	Yes. Mapped	Yes
1.3.6.1.4.1.24019.1.1.1.19	id-variant-highHardware	Yes. Mapped	Yes
1.3.6.1.4.1.24019.1.1.1.20	id-variant-mediumCBPSoftware	Yes. Mapped	No
1.3.6.1.4.1.24019.1.1.1.21	id-variant-mediumCBPHardware	Yes. Mapped	No
1.3.6.1.4.1.24019.1.1.1.22	id-variant-highCBPHardware	Yes. Mapped	No

6.13 Entrust Managed Services NFI PKI Assurance Levels

Entrust NFI PKI currently has a two-way cross-certificate relationship with the SHA-256 FBCA. It currently asserts the following certificate policies in its certificates, five of which are permitted by DoD policy:

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
2.16.840.1.114027.200.3.10.7.1	id-emspki-nfssp-medium-policy	Yes. Mapped	No
2.16.840.1.114027.200.3.10.7.2	id-emspki-nfssp-medium-hardware	Yes. Mapped	Yes
2.16.840.1.114027.200.3.10.7.3	id-emspki-nfssp-medium-devices	Yes. Mapped	No
2.16.840.1.114027.200.3.10.7.4	id-emspki-nfssp-mediumauthentication	Yes. Mapped	Yes
2.16.840.1.114027.200.3.10.7.5	id-emspki-nfssp-medium-cardAuth	Yes. Mapped	Yes-Physical access only
2.16.840.1.114027.200.3.10.7.6	id-emspki-nfssp-pivi-hardware	Yes. Mapped	Yes
2.16.840.1.114027.200.3.10.7.7	id-emspki-nfssp-basic-policy	Yes. Mapped	No
2.16.840.1.114027.200.3.10.7.8	id-emspki-nfssp-rudimentary-policy	Yes. Mapped	No
2.16.840.1.114027.200.3.10.7.9	id-emspki-nfssp-pivi-contentsigning	Yes. Mapped	Yes
2.16.840.1.114027.200.3.10.8.1	id-emspki-safeca-basic	No	No
2.16.840.1.114027.200.3.10.8.2	id-emspki-safeca-medium-software	No	No
2.16.840.1.114027.200.3.10.8.3	id-emspki-safeca-medium-hardware	No	No

[30] CertiPath has additional OIDs that are obsolete, reserved, or used for test purposes. CertiPath lists the entire arc here: http://www.certipath.com/downloads/CertiPath%20CP-v.3.26_final.pdf

6.14 Exostar Assurance Levels

Exostar Federated Identity Service Root CA 2 currently has a two-way cross-certificate relationship with the SHA-256 Federal Bridge CA. It currently asserts the following certificate policies in its certificates, one of which is permitted by DoD policy:

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
1.3.6.1.4.1.13948.1.1.1.5	id-mediumSoftware-sha2	Yes. Mapped	No
1.3.6.1.4.1.13948.1.1.1.6	id-mediumHardware-sha2	Yes. Mapped	Yes
1.3.6.1.4.1.13948.1.1.1.8	id-basic-sha2	Yes. Mapped	No

6.15 IdenTrust NFI PKI Assurance Levels

IdenTrust Global Common Root CA currently has a two-way cross-certificate relationship with the SHA-256 Federal Bridge CA. It currently asserts the following certificate policies in its certificates, seven of which are permitted by DoD policy:

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
2.16.840.1.113839.0.100.2.1	id-igc-BasicSoftware-SigningCertificate	Yes. Mapped	No
2.16.840.1.113839.0.100.2.2	id-igc-BasicSoftware-Encryption Certificate	Yes. Mapped	No
2.16.840.1.113839.0.100.3.1	id-igc-MediumSoftware-SigningCertificate	Yes. Mapped	No
2.16.840.1.113839.0.100.3.2	id-igc-MediumSoftware-EncryptionCertificate	Yes. Mapped	No
2.16.840.1.113839.0.100.12.1	id-igc-MediumHardware-SigningCertificate	Yes. Mapped	Yes
2.16.840.1.113839.0.100.12.2	id-igc-MediumHardware-EncryptionCertificate	Yes. Mapped	Yes
2.16.840.1.113839.0.100.14.1	id-igc-MediumCommercialBestPractices-SigningCertificate	Yes. Mapped	No
2.16.840.1.113839.0.100.14.2	id-igc-MediumCommercialBest Practices-EncryptionCertificate	Yes. Mapped	No
2.16.840.1.113839.0.100.15.1	id-igc-MediumHardwareCommercialBestPractices-SigningCertificate	Yes. Mapped	No
2.16.840.1.113839.0.100.15.2	id-igc-MediumHardwareCommercialBestPractices-EncryptionCertificate	Yes. Mapped	No
2.16.840.1.113839.0.100.18.0	id-igc-pivi-hardware-identity	Yes. Mapped	Yes
2.16.840.1.113839.0.100.18.1	id-igc-pivi-hardware-signing	Yes. Mapped	Yes
2.16.840.1.113839.0.100.18.2	id-igc-pivi-hardware-encryption	Yes. Mapped	Yes
2.16.840.1.113839.0.100.19.1	id-igc-pivi-CardAuthentication	Yes. Mapped	Yes
2.16.840.1.113839.0.100.20.1	id-igc-pivi-contentSigning	Yes. Mapped	Yes
2.16.840.1.113839.0.100.37.1	id-igc-MediumDeviceSoftware-DeviceCertificate	No	No

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
2.16.840.1.113839.0.100.37.2	id-igc-MediumDeviceSoftware-SSLcertificate	No	No
2.16.840.1.113839.0.100.38.1	id-igc-MediumDeviceHardware-DeviceCertificate	No	No
2.16.840.1.113839.0.100.38.2	id-igc-MediumDeviceHardware-SSLcertificate	No	No

6.16 Lockheed Martin Assurance Levels

Lockheed Martin currently has a two-way cross-certificate relationship with the SHA-1 CertiPath Bridge CA. The SHA-1 CertiPath Bridge CA has a two-way cross-certificate relationship with the SHA-1 Federal Root CA. Lockheed Martin currently asserts the following certificate policies in its certificates, one of which is permitted by DoD policy:

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
1.3.6.1.4.1.103.100.1.1.3.1	id-variant-mediumHardware	Yes. Mapped	Yes
1.3.6.1.4.1.103.100.1.1.3.2	id-variant-mediumSoftware	Yes. Mapped	No
1.3.6.1.4.1.103.100.1.1.3.3	Medium Assurance Hardware Certificate	Yes. Mapped	Yes
1.3.6.1.4.1.103.100.1.1.3.4	Medium Assurance Software Certificate	Yes. Mapped	No

6.17 Netherlands Ministry of Defence PKI Assurance Levels

The Netherlands Ministry of Defence PKI currently has a two-way cross-certificate relationship with the CertiPath Bridge CA – G2 (SHA-256). It currently asserts the following certificate policies in its certificates, all of which are permitted by DoD policy:

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
2.16.528.1.1003.1.2.5.1	Authenticity	Yes. Mapped	Yes
2.16.528.1.1003.1.2.5.2	Irrefutability/signature	Yes. Mapped	Yes
2.16.528.1.1003.1.2.5.3	Confidentiality	Yes. Mapped	Yes

6.18 Northrop Grumman PKI Assurance Levels

Northrop Grumman Corporation Root CAs currently has a two-way cross-certificate relationship with the SHA-1 CertiPath Bridge CA for their SHA-1 PKI and a two-way cross-certificate relationship with the SHA-256 CertiPath Bridge CA – G2 for their SHA-256 PKI. It currently asserts the following certificate policies in its certificates, five of which are permitted by DoD policy:

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
1.3.6.1.4.1.16334.509.2.5	Northrop Grumman Enterprise Medium Assurance-Software	Yes. Mapped	No
1.3.6.1.4.1.16334.509.2.6	Northrop Grumman Enterprise Medium Assurance-Hardware	Yes. Mapped	Yes
1.3.6.1.4.1.16334.509.2.7	Medium Assurance-256 Software Certificate	Yes. Mapped	No
1.3.6.1.4.1.16334.509.2.8	Medium Assurance-256 Hardware Token	Yes. Mapped	Yes
1.3.6.1.4.1.16334.509.2.9	PIV-I Assurance-256 Hardware Token	Yes. Mapped	Yes

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
1.3.6.1.4.1.16334.509.2.10	PIV-I Assurance-256 Card Authentication	Yes. Mapped	Yes. Physical Access Only
1.3.6.1.4.1.16334.509.2.11	PIV-I Assurance-256 Content Signing	Yes. Mapped	Yes

6.19 ORC NFI PKI Assurance Levels

ORC NFI CA 2 has a two-way cross-certificate relationship with the Federal Bridge CA. ORC NFI currently asserts the following certificate policies in its certificates, four of which are permitted by DoD policy:

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
1.2.840.113549.5.6.1.3.1.3	id-orc-nfissp-medium	Yes	No
1.2.840.113549.5.6.1.3.1.12	id-orc-nfissp-mediumhardware	Yes	Yes
1.2.840.113549.5.6.1.3.1.18	id-orc-nfissp-pivi-hardware	Yes	Yes
1.2.840.113549.5.6.1.3.1.19	id-orc-nfissp-pivi-cardAuth	Yes	Yes – Physical Access Only
1.2.840.113549.5.6.1.3.1.20	id-orc-nfissp-pivi-contentSigning	Yes	Yes
1.2.840.113549.5.6.1.3.1.21	id-orc-nfissp-devices	Yes	No

6.20 Raytheon PKI Assurance Levels

Raytheon currently has a two-way cross-certificate relationship with the SHA-1 and SHA-256 CertiPath Bridge CAs. It has multiple assurance levels defined below. It currently asserts the following certificate policies in its certificates, three of which are permitted by DoD policy:

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
1.3.6.1.4.1.1569.10.1.1	id-raytheon-SHA1-high	Yes. Mapped	Yes
1.3.6.1.4.1.1569.10.1.2	id-raytheon-SHA1-mediumHardware	Yes. Mapped	Yes
1.3.6.1.4.1.1569.10.1.3	id-raytheon-SHA1-mediumSoftware	Yes. Mapped	No
1.3.6.1.4.1.1569.10.1.4	id-raytheon-SHA1-mediumCBPHardware	Yes. Mapped	No
1.3.6.1.4.1.1569.10.1.5	id-raytheon-SHA1-mediumCBPSoftware	Yes. Mapped	No
1.3.6.1.4.1.1569.10.1.6	id-raytheon-lowHardware	No	No
1.3.6.1.4.1.1569.10.1.7	id-raytheon-lowSoftware	No	No
1.3.6.1.4.1.1569.10.1.11	id-raytheon-high	No	No
1.3.6.1.4.1.1569.10.1.12	id-raytheon-mediumHardware	Yes. Mapped	Yes
1.3.6.1.4.1.1569.10.1.13	id-raytheon-mediumSoftware	No	No
1.3.6.1.4.1.1569.10.1.14	id-raytheon-mediumCBPHardware	No	No
1.3.6.1.4.1.1569.10.1.15	id-raytheon-mediumCBPSoftware	No	No
1.3.6.1.4.1.1569.10.1.20	id-raytheon-test	No	No

6.21 Symantec NFI PKI Assurance Levels

Symantec NFI PKI currently has a two-way cross-certificate relationship with the SHA-256 FBCA. Symantec NFI PKI currently asserts the following certificate policies in its certificates, six of which are permitted by DoD policy:

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
2.16.840.1.113733.1.7.23.3.1.6	Non-Federal SSP Medium	Yes. Mapped	No
2.16.840.1.113733.1.7.23.3.1.7	Non-Federal SSP MediumHardware	Yes. Mapped	Yes
2.16.840.1.113733.1.7.23.3.1.8	Non-Federal SSP Devices	Yes. Mapped	No
2.16.840.1.113733.1.7.23.3.1.13 (no longer issued, found in legacy certificates only)	Non-Federal SSP Auth	Yes. Mapped	Yes
2.16.840.1.113733.1.7.23.3.1.14	Non-Federal SSP Medium CBP	Yes. Mapped	No
2.16.840.1.113733.1.7.23.3.1.15	Non-Federal SSP MediumHardware CBP	Yes. Mapped	No
2.16.840.1.113733.1.7.23.3.1.17	Non-Federal SSP PIV-I cardAuth	Yes. Mapped	Yes – Physical Access Only
2.16.840.1.113733.1.7.23.3.1.18	Non-Federal SSP PIV-I Hardware	Yes. Mapped	Yes
2.16.840.1.113733.1.7.23.3.1.20	Non-Federal SSP PIV-I contentSigning	Yes. Mapped	Yes
2.16.840.1.113733.1.7.23.3.1.36	Non-Federal SSP mediumDevicesHardware	Yes. Mapped	Yes

6.22 TSCP SHA-256 Bridge Assurance Levels

TSCP is an organization that provides bridge services and has one bridge CA that is cross certified with the Federal Bridge CA. TSCP vets and cross-certifies commercial and Aero/Defense partners to include PIV-Interoperable (PIV-I) partners.

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
1.3.6.1.4.1.38099.1.1.1.1	id-Medium	No	No
1.3.6.1.4.1.38099.1.1.1.2	id-MediumHardware	Yes. Mapped	Yes
1.3.6.1.4.1.38099.1.1.1.3	id-Medium-CBP	No	No
1.3.6.1.4.1.38099.1.1.1.4	id-MediumHardware-CBP	No	No
1.3.6.1.4.1.38099.1.1.1.5	id-PIVI	Yes. Mapped	Yes
1.3.6.1.4.1.38099.1.1.1.6	id-PIVI-CardAuth	Yes. Mapped	Yes
1.3.6.1.4.1.38099.1.1.1.7	id-PIVI-ContentSigning	Yes. Mapped	Yes
1.3.6.1.4.1.38099.1.1.1.8	id-SHA1-Medium	No	No
1.3.6.1.4.1.38099.1.1.1.9	id-SHA1-MediumHardware	No	No
1.3.6.1.4.1.38099.1.1.1.10	id-SHA1-Medium-CBP	No	No
1.3.6.1.4.1.38099.1.1.1.11	id-SHA1-MediumHardware-CBP	No	No

6.23 Verizon Business NFI PKI Assurance Levels

Verizon Business NFI PKI currently has a two-way cross-certificate relationship with the Federal Bridge CA. It currently asserts the following certificate policies in its certificates, four of which are permitted by DoD policy:

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
1.3.6.1.4.1.23337.1.1.1	id-Cybertrust-Commercial-CBP-Software	Yes. Mapped	No

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
1.3.6.1.4.1.23337.1.1.2	id-Cybertrust-Commercial-CBP-Hardware	Yes. Mapped	No
1.3.6.1.4.1.23337.1.1.3	id-Cybertrust-Commercial-CBP-Devices	Yes. Mapped	No
1.3.6.1.4.1.23337.1.1.4	id-Cybertrust-Commercial-CBP-Authentication	Yes. Mapped	No
1.3.6.1.4.1.23337.1.1.5	id-Cybertrust-Commercial-CBP-Basic	Yes. Mapped	No
1.3.6.1.4.1.23337.1.1.6	id-Cybertrust-Commercial-CBP-cardAuthentication	Yes. Mapped	No
1.3.6.1.4.1.23337.1.1.7	id-Cybertrust-Software	Yes. Mapped	No
1.3.6.1.4.1.23337.1.1.8	id-Cybertrust-Hardware	Yes. Mapped	Yes
1.3.6.1.4.1.23337.1.1.9	id-Cybertrust-Devices	Yes. Mapped	No
1.3.6.1.4.1.23337.1.1.10	id-Cybertrust-Authentication	Yes. Mapped	Yes
1.3.6.1.4.1.23337.1.1.11	Id-Cybertrust-contentSigner	Yes. Mapped	Yes
1.3.6.1.4.1.23337.1.1.12	id-Cybertrust-cardAuthentication	Yes. Mapped	Yes-Physical access only

6.24 Australian Defence Organisation (ADO) PKI Assurance Levels

ADO currently has a two-way cross-certificate relationship with the US DoD CCEB Interoperability Root CA 1. It currently asserts the following certificate policies in its certificates, three of which are permitted by DoD policy:

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO DoD (Y/N)	ALLOWABLE PER CCA (Y/N)
1.2.36.1.334.1.2.1.1	ADO Individual Low Assurance	No	No
1.2.36.1.334.1.2.1.2	ADO Individual Medium Assurance	Yes. Mapped	Yes
1.2.36.1.334.1.2.1.3	ADO Individual High Assurance	No	No
1.2.36.1.334.1.2.1.4	ADO Individual Very High Assurance	No	No
1.2.36.1.334.1.2.2.1	ADO Resource Low Assurance	Yes. Mapped	Yes
1.2.36.1.334.1.2.2.2	ADO Resource Medium Assurance	Yes. Mapped	Yes
1.2.36.1.334.1.2.2.3	ADO Resource High Assurance	No	No

Glossary of Terms[31]

Access Control The process of granting or denying specific requests: 1) for obtaining and using information and related information processing services; and 2) to enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances).

Access Control mechanism Security safeguards (i.e., hardware and software features, physical controls, operating procedures, management procedures, and various combinations of these) designed to detect and deny unauthorized access and permit authorized access to an information system.

Assurance Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy.

Assurance Level The level of assurance refers to the strength of the binding between the public key and the individual whose subject name is cited in the certificate, the mechanisms used to control the use of the private key, and the security provided by the PKI itself.[32] In the context of this document, assurance levels are represented by Certificate Policy Object Identifiers (OIDs) which translate back to defined controls specified in corresponding organizational or Federal PKI Certificate Policy documents.

Authenticate To verify the identity of a user, user device, or other entity.

Authentication Hardware or software-based algorithm that forces users, devices, or processes to prove their identity before accessing data on an information system.

Authorization Access privileges granted to a user, program, or process or the act of granting those privileges.

Category I PKI U.S. Federal Agency PKI.

Category II PKI Non-Federal Agency PKIs cross certified with the FBCA or PKIs from other PKI Bridges that are cross certified with the FBCA

Category III PKI Foreign, Allied, or Coalition Partner PKIs or other PKI

Certification Authority A trusted third party that issues digital certificates and verifies the identity of the holder of the digital certificate.

[31] Definitions were largely taken directly from the National Information Assurance Glossary, CNSS- 4009 https://www.cnss.gov/CNSS/issuances/Instructions.cfm. Some definitions were taken from CIO Council *Personal Identity Verification (PIV) Interoperability For Non-Federal Issuers* document. Full text and requirements are available here: https://www.idmanagement.gov/IDM/s/document_detail?Id=kA0t00000008OfMCAU

[32] Assurance level definition taken from FBCA Certificate Policy document, https://www.idmanagement.gov/IDM/s/document_detail?Id=kA0t00000008OcKCAU

Certificate
A digitally signed representation of information that 1) identifies the authority issuing it, 2) identifies the subscriber, 3) identifies its valid operational period (date issued / expiration date).

Certificate Policy (CP)
A specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery, and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.

Certificate Revocation List (CRL)
A list of revoked public key certificates created and digitally signed by a Certification Authority.

Credential
Evidence or testimonials that support a claim of identity or assertion of an attribute and usually are intended to be used more than once.

Credential Service Provider (CSP)
A trusted entity that issues or registers subscriber tokens and issues electronic credentials to subscribers. The CSP may encompass registration authorities and verifiers that it operates. A CSP may be an independent third party, or may issue credentials for its own use.

Cross-certificate
A certificate used to establish a trust relationship between two Certification Authorities.

Digital Signature
Cryptographic process used to assure data object originator authenticity, data integrity, and time stamping for prevention of replay.

Direct Trust
Method of PKI trust where the relying party directly installs the trust anchor of another PKI. (Note: this does not mean cross-certificate trust is not inherited via transitive trust)

Distinguished Name (DN)
A unique name or character string that unambiguously identifies an entity according to the hierarchical naming conventions of X.500 directory service.

DoD CIO
Office of the Department of Defense (DoD) Chief Information Officer (CIO). Governing authority for DoD approved external PKIs.

Cross-certificate trust
Method of PKI trust where the relying party installs an internal trust anchor and inherits trust through issued cross-certificates.

Federal Bridge Certification Authority (FBCA)
See Federal PKI.

External Certification Authority (ECA)
DoD program to support the issuance of DoD-approved certificates to industry partners and other external entities and organizations.

Federal Information Processing Standard (FIPS)
A standard for adoption and use by Federal agencies that has been developed within the Information Technology Laboratory and published by the National Institute of Standards

and Technology, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology in order to achieve a common level of quality or some level of interoperability.

Federal Public Key Infrastructure (Federal PKI or FPKI)

The Federal PKI consists of a collection of Public Key Infrastructure components (Certificate Authorities, Directories, Certificate Policies and Certificate Practice Statements) that are used to provide peer-to-peer interoperability and a Federal Trust Anchor for SSP PKIs.

In the context of this document there are five specific FPKI systems.

1. Legacy FBCA (ou=Entrust). Legacy FBCA system that is being decommissioned on 6/30/11.
2. Legacy Common Policy. The old Federal trust anchor and former parent for Shared Service Provider PKIs. It is to be decommissioned on 6/30/11.
3. SHA-1 Federal Root CA. This system is the new SHA-1 trust anchor and bridge CA that cross certifies other SHA-1 bridge member CAs and provides a Federal trust anchor for some SHA-1 legacy SSP PKIs.
4. Federal Bridge CA (FBCA). New SHA-256 FBCA system that cross certifies with other SHA-256 bridge member CAs.
5. Federal Common Policy CA. SHA-256 trust anchor for most of the Federal Government to include SSP PKIs. It also issues cross-certificates to some legacy PKIs.

Federal PKI Policy Authority (FPKI PA)

The Federal Public Key Infrastructure (FPKI) Policy Authority is an interagency body set up under the CIO Council to enforce digital certificate standards for trusted identity authentication across the federal agencies and between federal agencies and outside bodies, such as universities, state and local governments and commercial entities.

Global Directory Service (GDS)

DoD directory service that hosts all CA information to include CA certificates, cross-certificate content, and CRLs. GDS provides both a web and directory service. GDS hosts CA information at via HTTP/HTTPS at crl.disa.mil and via LDAP at crl.gds.disa.mil. GDS also hosts user encryption certificates at https://dod411.gds.disa.mil.

Legacy PKI

Agency-operated PKI that was in existence prior to Jan 1, 2008.[33]

Memorandum of Agreement (MOA)

Binding agreement between DoD Policy Management Authority and the External PKI. Required for Category I or Category II PKIs.

Non-Federal Issuer

A PKI or Card issuer that is not a Federal PIV issuer.

[33] FIPS 201 describes Legacy PKI requirements and is available at http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf

Online Certificate Status Protocol (OCSP)
Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate and is described in RFC 2560.

Personal Identity Verification (PIV)
The process of creating and using a government-wide secure and reliable form of identification for Federal employees and contractors, in support of HSPD 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*.

Personal Identity Verification (PIV) Card
A government-issued credit card-sized identification that contains a contact and contactless chip. The holder's facial image will be printed on the card, along with other identifying information and security features. The contact chip will store a PKI certificate, the Cardholder Unique Identifier (CHUID), and a fingerprint biometric, all of which can be used to authenticate the user for physical access to federally controlled facilities and logical access to federally-controlled information systems. A PIV Card is fully conformant with federal PIV standards (i.e., Federal Information Processing Standard (FIPS) 201 and related documentation). Only cards issued by federal entities can be fully conformant. Federal standards ensure the PIV Cards are interoperable with and trusted by all Federal government relying parties.

PIV-Interoperable (PIV-I)
The process of creating and using a secure and reliable form of identification that is interoperable with the Federal government PIV process.[34]

PIV Interoperable (PIV-I) Card
A PIV-I (Personal Identity Verification – Interoperable) Card meets the PIV technical specifications to work with Federal PIV infrastructure elements such as card readers, and is issued in a manner that allows Federal government Relying Parties to trust the card. The PIV-I Card is suitable for level of assurance 4 as defined in OMB Memorandum M-04-04 and NIST SP 800-63, as well as multi-factor authentication as defined in NIST SP 800-116. A PIV-I card differs from a PIV card in that it does not meet all the requirements of FIPS-201.[35]

Public Key
A cryptographic key that may be widely published and is used to enable the operation of an asymmetric cryptography scheme. This key is mathematically linked with a corresponding private key. Typically, a public key can be used to encrypt, but not decrypt, or to validate a signature, but not to sign.

Public Key Enabling (PKE)
The incorporation of the use of PKI certificates for security services such as authentication, confidentiality, data integrity, and non-repudiation.

Public Key Infrastructure (PKI)
The framework and services that provide for the generation, production, distribution, control, accounting and destruction of public key certificates. Components include the personnel, policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, recover, and revoke public key certificates.

Relying party
An entity that relies upon the subscriber's credentials, typically to process a transaction or grant access to information or a system

[34] The PIV-I certification process is detailed at https://www.idmanagement.gov/IDM/s/document_detail?Id=kA0t00000008OfjCAE

[35] PIV-I FAQ available at https://www.idmanagement.gov/IDM/s/document_detail?Id=kA0t00000008OcOCAU

Robust Certificate Validation Service (RCVS) DoD service that provides certificate validation information to DoD PKI relying parties to include OCSP responses.

Root Certification Authority In a hierarchical Public Key Infrastructure, the Certification Authority whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.

Shared Service Provider[36] Entity authorized by Federal PKI PA to perform CA services for Agencies.

Subordinate Certification Authority In a hierarchal PKI, a Certification Authority whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA.

Subscriber A party who receives a credential or token from a Credentials Service Provider (CSP) and becomes a claimant in an authentication protocol.

Transitive Trust Term used to describe trust inherited from direct trust implementations. An implementation example would be installing another PKI trust anchor which has issued a cross-certificate outside its own PKI.

Trust Anchor An established point of trust (usually based on the authority of some person, office, or organization) from which an entity begins the validation of an authorized process or authorized (signed) package. A "trust anchor" is sometimes defined as just a public key used for different purposes (e.g., validating a Certification Authority, validating a signed software package or key, validating the process (or person) loading the signed software or key).

Unclassified Information that has not been determined pursuant to E.O. 12958, as amended, or any predecessor order, to require protection against unauthorized disclosure and that is not designated as classified.

User Individual, or (system) process acting on behalf of an individual, authorized to access an information system

Validation Confirmation (through the provision of strong, sound, objective evidence) that requirements for a specific intended use or application have been fulfilled (e.g., a trustworthy credential has been presented, or data or information has been formatted in accordance with a defined set of rules, or a specific process has demonstrated that an entity under consideration meets, in all respects, its defined attributes or requirements).

X.509 Public Key Certificate The public key for a user (or device) and a name for the user (or device), together with some other information, rendered unforgeable by the digital signature of the certification authority that issued the certificate, encoded in the format defined in the ISO/ITU-T X.509 standard. Also known as X.509 Certificate.

[36] Official list of certified Shared Service Providers is available at https://www.idmanagement.gov/IDM/s/article_content_old?tag=a0Gt0000000XRrC.